



UTM Guide

FortiOS™ Handbook v4.3
for FortiOS 4.0 MR3



FortiOS™ Handbook UTM Guide

v3

12 September 2013

01-4310-108920-20130912

Copyright© 2012 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Visit these links for more information and documentation for your Fortinet products:

Fortinet Knowledge Base - <http://kb.fortinet.com>

Technical Documentation - <http://docs.fortinet.com>

Training Services - <http://campus.training.fortinet.com>

Technical Support - <http://support.fortinet.com>

You can report errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.

Introduction	13
Before you begin	13
How this chapter is organized	13
UTM overview	15
UTM components	15
AntiVirus	15
Intrusion Protection System (IPS)	15
Anomaly protection (DoS policies)	16
One-armed IDS (sniffer policies)	16
Web filtering	16
Email filtering	16
Data Leak Prevention (DLP)	16
Application Control (for example, IM and P2P)	16
UTM profiles/lists/sensors	17
Network defense	19
Monitoring	19
Blocking external probes	19
Address sweeps	20
Port scans	20
Probes using IP traffic options	20
Evasion techniques.	22
Defending against DoS attacks	24
The “three-way handshake”	24
SYN flood	24
SYN spoofing.	25
DDoS SYN flood	26
Configuring the SYN threshold to prevent SYN floods	26
SYN proxy	26
Other flood types.	27
Traffic inspection	27
IPS signatures	27
Suspicious traffic attributes	28
DoS policies	28
Application control	28
Content inspection and filtering	29
AntiVirus	29
FortiGuard Web Filtering	29
Email filter	30
DLP.	30

AntiVirus	31
Antivirus concepts	31
How antivirus scanning works	31
Antivirus scanning order	32
Antivirus databases	34
Antivirus techniques	35
FortiGuard Antivirus	35
Enable antivirus scanning	36
Viewing antivirus database information	36
Changing the default antivirus database.	36
Overriding the default antivirus database	37
Adding the antivirus profile to a security policy	38
Configuring the scan buffer size	38
Configuring archive scan depth	38
Configuring a maximum allowed file size	39
Configuring client comforting	40
Enable the file quarantine.	41
General configuration steps	41
Configuring the file quarantine	41
Viewing quarantined files.	42
Downloading quarantined files.	42
Enable grayware scanning	42
Testing your antivirus configuration	42
Antivirus examples	43
Configuring simple antivirus protection	43
Protecting your network against malicious email attachments	44
AntiVirus interface reference	45
Profile.	46
Virus Database	47
Email filter	49
Email filter concepts	49
Email filter techniques	49
Order of spam filtering	51
Enable email filter.	52
Configure email traffic types to inspect	52
Configure the spam action	52
Configure the tag location	53
Configure the tag format	53

Configure FortiGuard email filters	54
Enabling FortiGuard IP address checking	54
Enabling FortiGuard URL checking	54
Enabling FortiGuard phishing URL detection	54
Enabling FortiGuard email checksum checking	55
Enabling FortiGuard spam submission	55
Configure local email filters.	56
Enabling IP address black/white list checking	56
Enabling HELO DNS lookup	57
Enabling email address black/white list checking	58
Enabling return email DNS checking.	59
Enabling banned word checking.	59
How content is evaluated	60
Email filter examples	62
Configuring simple antispam protection	62
Blocking email from a user.	63
Email Filter interface reference	64
Profile.	66
Banned Word.	69
IP Address	72
E-mail Address.	75
Intrusion protection	79
IPS concepts	79
Anomaly-based defense	79
Signature-based defense	79
Enable IPS scanning	81
General configuration steps	81
Creating an IPS sensor.	81
Creating an IPS filter	81
Filter order	84
Updating predefined IPS signatures	84
Viewing and searching predefined IPS signatures.	84
Creating a custom IPS signature.	85
Custom signature syntax and keywords	86
IPS processing in an HA cluster	100
Active-passive	100
Active-active	101

Configure IPS options	101
Configuring the IPS engine algorithm	101
Configuring the IPS engine-count	101
Configuring fail-open.	101
Configuring the session count accuracy	101
Configuring the IPS buffer size.	102
Configuring security processing modules	102
Enable IPS packet logging	102
IPS examples	103
Configuring basic IPS protection.	103
Using IPS to protect your web server	104
Create and test a packet logging IPS sensor	106
Creating a custom signature to block access to example.com	108
Creating a custom signature to block the SMTP “vrfy” command	109
Configuring a Fortinet Security Processing module	111
Intrusion Protection interface reference	115
IPS Sensor	115
DoS sensor.	122
Predefined	126
Custom.	130
Protocol Decoder	131
Web filter	133
Before you begin	133
The following topics are included in this section:	133
Web filter concepts.	133
Different ways of controlling access	135
Order of web filtering.	135
Web content filter.	135
General configuration steps	136
Creating a web filter content list	136
How content is evaluated	137
Enabling the web content filter and setting the content threshold.	138
URL filter	139
URL filter actions.	139
General configuration steps	141
Creating a URL filter list	141
Configuring a URL filter list.	141
SafeSearch	141

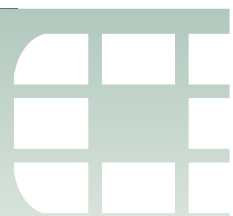
Advanced web filter configuration	142
ActiveX filter	142
Cookie filter.	142
Java applet filter	142
Web resume download block	142
Block Invalid URLs	143
HTTP POST action	143
Web filtering example	143
School district	144
Web Filter interface reference	147
Profile.	147
Browser cookie-based FortiGuard Web Filtering overrides	152
URL Filter.	153
Local Ratings.	157
FortiGuard Web Filter	159
Before you begin	159
FortiGuard Web Filter and your FortiGate unit	160
Order of web filtering.	160
Enable FortiGuard Web Filter.	162
General configuration steps	162
Configuring FortiGuard Web Filter settings	162
Configuring FortiGuard Web Filter usage quotas	163
Checking quota usage	165
Advanced FortiGuard Web Filter configuration	165
Provide Details for Blocked HTTP 4xx and 5xx Errors.	165
Rate Images by URL (blocked images will be replaced with blanks)	165
Allow Websites When a Rating Error Occurs	166
Strict Blocking	166
Rate URLs by Domain and IP Address	166
Block HTTP Redirects by Rating.	166
Daily log of remaining quota	167
Add or change FortiGuard Web Filter ratings	167
Create FortiGuard Web Filter overrides	167
Understanding administrative and user overrides	167
Customize categories and ratings	168
Creating local categories.	168
Customizing site ratings	168
FortiGuard Web Filter examples	168
Configuring simple FortiGuard Web Filter protection	169
School district	170

Data leak prevention	171
Data leak prevention concepts	171
DLP sensor	171
DLP filter	171
Fingerprint	172
File filter	172
File size.	172
Regular expression.	172
Advanced rule	172
Compound rule.	172
Enable data leak prevention	172
General configuration steps	172
Creating a DLP sensor	173
Adding filters to a DLP sensor	173
DLP document fingerprinting.	176
Fingerprinted Documents	177
File filter.	178
General configuration steps	178
Creating a file filter list	179
Creating a file pattern	179
Creating a file type	179
Advanced rules	180
Understanding the default advanced rules	180
Creating advanced rules	181
Compound rules	181
Understanding the default compound rules	181
Creating compound rules	182
DLP archiving.	182
DLP examples	183
Blocking sensitive email messages	183
Data Leak Prevention interface reference	185
Sensor	185
Document Fingerprinting.	190
File Filter	192
DLP archiving	196
Application control	197
Application control concepts.	197

Enable application control	198
General configuration steps	198
Creating an application sensor.	198
Adding applications to an application sensor	198
Understanding the default application sensor	202
Viewing and searching the application list	202
Application traffic shaping	203
Enabling application traffic shaping	203
Reverse direction traffic shaping.	204
Shaper re-use	204
Application control monitor.	205
Enabling application control monitor.	205
Application control packet logging	206
Application considerations	207
IM applications	207
Skype.	207
Application control examples.	207
Blocking all instant messaging.	207
Allowing only software updates	208
Application Control interface reference	209
Application Sensor	210
Application List.	214
DoS policy	217
DoS policy concepts	217
Enable DoS.	217
Creating and configuring a DoS sensor	218
Creating a DoS policy	219
Apply an IPS sensor to a DoS policy.	220
DoS example	220
DoS Policy interface reference	221
Endpoint Control and monitoring	225
Endpoint Control overview	225
User experience	225
Configuration overview.	227
Configuring FortiClient required version and download location.	227
About application detection and control	229
FortiClient application rules	229
Other application rules	229
The All application rule.	229
About predefined profiles.	230

Creating an endpoint control profile	230
Setting endpoint FortiClient requirements	230
Setting the default action for applications	232
Adding application detection entries.	232
Viewing the application database	233
Enabling Endpoint Control in firewall policies	234
Monitoring endpoints.	235
Endpoint status	235
Endpoint Application Usage	236
Endpoint Traffic	236
Modifying Endpoint Security replacement pages	236
Example	237
Configuring FortiClient download source and required version	237
Creating an endpoint control profile	238
Configuring FortiClient application detection entries	238
Configuring application detection entries for other applications	238
Configuring the firewall policy	240
Endpoint Control interface reference.	240
Profile.	241
Application Database	243
Client Installers.	246
Vulnerability Scan	249
Overview	249
Selecting assets to scan	249
Discovering assets	249
Adding assets manually	250
Requirements for authenticated scanning	252
Configuring scans	253
Viewing scan results	257
Viewing scan logs	257
Viewing Executive Summary graphs.	258
Creating reports	258
Viewing reports.	259
Vulnerability Scan interface reference	259
Asset Definition.	260
Scan Schedule	261
Vulnerability Result.	262
Sniffer policy	263
Sniffer policy concepts	263
The sniffer policy list	263
Before you begin	264

Enable one-arm sniffing	265
General configuration steps	265
Designating a sniffer interface	266
Creating a sniffer policy	266
Sniffer example	267
An IDS sniffer configuration	267
Sniffer Policy interface reference	270
Other UTM considerations	273
UTM and Virtual domains (VDOMs)	273
Conserve mode.	273
The AV proxy	273
Entering and exiting conserve mode.	274
Conserve mode effects	274
Configuring the av-failopen command.	275
SSL content scanning and inspection	275
Setting up certificates to avoid client warnings	276
SSL content scanning and inspection settings	277
Viewing and saving logged packets	280
Configuring packet logging options	280
Using wildcards and Perl regular expressions	281
Protocol Options interface reference.	284
Offloading UTM processing using Internet Content Adaptation Protocol (ICAP)	287
Example of adding ICAP to a security policy	287
Troubleshooting ICAP	288
ICAP profile.	288
ICAP server.	289
Profile Group interface reference.	289
Profile Group configuration settings	289
Monitor interface reference.	291
AV Monitor	291
Intrusion Monitor	292
Web Monitor	292
Email Monitor.	293
Archive & Data Leak Monitor.	293
Application Monitor	294
FortiGuard Quota.	294
Endpoint Monitor.	295
Index	297



Introduction

Welcome and thank you for selecting Fortinet products for your network protection.

FortiOS Handbook: UTM describes the Unified Threat Management (UTM) features available on your FortiGate unit, including antivirus, intrusion prevention system (IPS), anomaly protection (DoS), one-armed IPS (sniffer policies), web filtering, email filtering, data leak prevention, (DLP) and application control. The guide includes step-by-step instructions showing how to configure each feature. Example scenarios are included, with suggested configurations.

Examples include school scenarios using web filtering to protect students from inappropriate content, using IPS and DoS sensors to protect web servers from attack, and using antivirus scanning to protect your network against viruses and malicious file attachments.

This section contains the following topics:

- [Before you begin](#)
- [How this chapter is organized](#)

Before you begin

Before you begin using this guide, take a moment to note the following:

- Administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.
- Firewall policies limit access, and, while this and other similar features are a vital part of securing your network, they are not covered in this guide.
- If your FortiGate unit supports SSL acceleration, it also supports SSL content scanning and inspection for HTTPS, IMAPS, POP3S, and SMTPS traffic.

How this chapter is organized

This FortiOS Handbook chapter contains the following sections:

[UTM overview](#) describes UTM components and their relation to firewall policies, as well as SSL content scanning and inspection. We recommend starting with this section to become familiar with the different features in your FortiGate unit.

[Network defense](#) explains basic denial of service (DoS) and distributed denial of service (DDOS) concepts and provides an overview of the best practices to use with all the UTM features to defend your network against infection and attack.

[AntiVirus](#) explains how the FortiGate unit scans files for viruses and describes how to configure the antivirus options.

[Email filter](#) explains how the FortiGate unit filters email, describes how to configure the filtering options and the action to take with email detected as spam.

[Intrusion protection](#) explains basic Intrusion Protection System (IPS) concepts and how to configure IPS options; includes guidance and a detailed table for creating custom signatures as well as several examples.

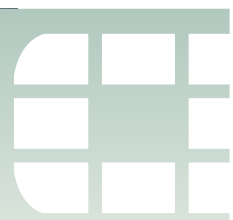
Web filter and **FortiGuard Web Filter** The first of these sections describes basic web filtering concepts, the order in which the FortiGate unit performs web filtering, and configuration. The second section describes enhanced features of the subscription-based FortiGuard Web Filtering service and explains how to configure them. We recommend reading both sections if you are using FortiGuard Web Filtering because settings you configure in one feature may affect the other.

Data leak prevention describes the DLP features that allow you to prevent sensitive data from leaving your network and explains how to configure the DLP rules, compound rules, and sensors.

Application control describes how your FortiGate unit can detect and take action against network traffic based on the application generating the traffic.

DoS policy describes how to use DoS policies to protect your network from DoS attacks.

Sniffer policy describes how to use your FortiGate unit as a one-armed intrusion detection system (IDS) to report on attacks.



UTM overview

Ranging from the FortiGate®-30 series for small businesses to the FortiGate-5000 series for large enterprises, service providers and carriers, the FortiGate line combines a number of security features to protect your network from threats. As a whole, these features, when included in a single Fortinet security appliance, are referred to as Unified Threat Management (UTM). The UTM features your FortiGate model includes are:

- AntiVirus
- Intrusion Prevention System (IPS)
- Anomaly protection (DoS policies)
- One-armed IPS (Sniffer policies)
- Web filtering
- E-mail filtering, including protection against spam and grayware
- Data Leak Prevention (DLP)
- Application Control (for example, IM and P2P).

Firewall policies limit access, and while this and similar features are a vital part of securing your network, they are not covered in this document.

The following topics are included in this section:

- [UTM components](#)
- [UTM profiles/lists/sensors](#)

UTM components

AntiVirus

Your FortiGate unit stores a virus signature database that can identify more than 15,000 individual viruses. FortiGate models that support additional virus databases are able to identify hundreds of thousands of viruses. With a FortiGuard AntiVirus subscription, the signature databases are updated whenever a new threat is discovered.

AntiVirus also includes file filtering. When you specify files by type or by file name, the FortiGate unit will stop the matching files from reaching your users.

FortiGate units with a hard drive or configured to use a FortiAnalyzer unit can store infected and blocked files for that you can examine later.

Intrusion Protection System (IPS)

The FortiGate Intrusion Protection System (IPS) protects your network against hacking and other attempts to exploit vulnerabilities of your systems. More than 3,000 signatures are able to detect exploits against various operating systems, host types, protocols, and applications. These exploits can be stopped before they reach your internal network.

You can also write custom signatures, tailored to your network.

Anomaly protection (DoS policies)

A complement to the signature-based IPS, anomaly protection detects unusual network traffic that can be used to attack your network. When you set thresholds for various types of network operations, the FortiGate unit will block any attempt to exceed the thresholds you have defined.

One-armed IDS (sniffer policies)

You can use sniffer policies on the FortiGate unit as a one-arm intrusion detection system (IDS). The unit examines traffic for matches to the configured IPS sensor and application control list. Matches are logged and then all received traffic is dropped. In this way, you can configure a unit to sniff network traffic for attacks without actually processing the packets.

The FortiGate unit can log all detected IPS signatures and anomalies in a traffic stream.

Web filtering

Web filtering includes a number of features you can use to protect or limit your users' activity on the web.

FortiGuard Web Filtering is a subscription service that allows you to limit access to web sites. More than 60 million web sites and two billion web pages are rated by category. You can choose to allow or block each of the 77 categories.

URL filtering can block your network users from access to URLs that you specify.

Web content filtering can restrict access to web pages based on words and phrases appearing on the web page itself. You can build lists of words and phrases, each with a score. When a web content list is selected in a web filter profile, you can specify a threshold. If a user attempts to load a web page and the score of the words on the page exceeds the threshold, the web page is blocked.

Email filtering

FortiGuard AntiSpam is a subscription service that includes an IP address black list, a URL black list, and an email checksum database. These resources are updated whenever new spam messages are received, so you do not need to maintain any lists or databases to ensure accurate spam detection.

You can use your own IP address lists and email address lists to allow or deny addresses, based on your own needs and circumstances.

Data Leak Prevention (DLP)

Data leak prevention allows you to define the format of sensitive data. The FortiGate unit can then monitor network traffic and stop sensitive information from leaving your network. Rules for U.S. social security numbers, Canadian social insurance numbers, as well as Visa, Mastercard, and American Express card numbers are included.

Application Control (for example, IM and P2P)

Although you can block the use of some applications by blocking the ports they use for communications, many applications do not use standard ports to communicate. Application control can detect the network traffic of more than 1000 applications, improving your control over application communication.

UTM profiles/lists/sensors

A profile is a group of settings that you can apply to one or more firewall policies. Each UTM feature is enabled and configured in a profile, list, or sensor. These are then selected in a security policy and the settings apply to all traffic matching the policy. For example, if you create an antivirus profile that enables antivirus scanning of HTTP traffic, and select the antivirus profile in the security policy that allows your users to access the World Wide Web, all of their web browsing traffic will be scanned for viruses.

Because you can use profiles in more than one security policy, you can configure one profile for the traffic types handled by a set of firewall policies requiring identical protection levels and types, rather than repeatedly configuring those same profile settings for each individual security policy.

For example, while traffic between trusted and untrusted networks might need strict protection, traffic between trusted internal addresses might need moderate protection. To provide the different levels of protection, you might configure two separate sets of profiles: one for traffic between trusted networks, and one for traffic between trusted and untrusted networks.

The UTM profiles include:

- antivirus profile
- IPS sensor
- Web filter profile
- Email filter profile
- Data Leak Prevention profile
- Application Control list
- VoIP profile

Although they're called profiles, sensors, and lists, they're functionally equivalent. Each is used to configure how the feature works.



Network defense

This section describes in general terms the means by which attackers can attempt to compromise your network and steps you can take to protect it. The goal of an attack can be as complex as gaining access to your network and the privileged information it contains, or as simple as preventing customers from accessing your web server. Even allowing a virus onto your network can cause damage, so you need to protect against viruses and malware even if they are not specifically targeted at your network.

The following topics are included in this section:

- [Monitoring](#)
- [Blocking external probes](#)
- [Defending against DoS attacks](#)
- [Traffic inspection](#)
- [Content inspection and filtering](#)

Monitoring

Monitoring, in the form of logging, alert email, and SNMP, does not directly protect your network. But monitoring allows you to review the progress of an attack, whether afterwards or while in progress. How the attack unfolds may reveal weaknesses in your preparations. The packet archive and sniffer policy logs can reveal more details about the attack. Depending on the detail in your logs, you may be able to determine the attackers location and identity.

While log information is valuable, you must balance the log information with the resources required to collect and store it.

Blocking external probes

Protection against attacks is important, but attackers often use vulnerabilities and network tools to gather information about your network to plan an attack. It is often easier to prevent an attacker from learning important details about your network than to defend against an attack designed to exploit your particular network.

Attacks are often tailored to the hardware or operating system of the target, so reconnaissance is often the first step. The IP addresses of the hosts, the open ports, and the operating systems the hosts are running is invaluable information to an attacker. Probing your network can be as simple as an attacker performing an address sweep or port scan to a more involved operation like sending TCP packets with invalid combinations of flags to see how your firewall reacts.

Address sweeps

An address sweep is a basic network scanning technique to determine which addresses in an address range have active hosts. A typical address sweep involves sending an ICMP ECHO request (a ping) to each address in an address range to attempt to get a response. A response signifies that there is a host at this address that responded to the ping. It then becomes a target for more detailed and potentially invasive attacks.

Address sweeps do not always reveal all the hosts in an address range because some systems may be configured to ignore ECHO requests and not respond, and some firewalls and gateways may be configured to prevent ECHO requests from being transmitted to the destination network. Despite this shortcoming, Address sweeps are still used because they are simple to perform with software tools that automate the process.

Use the `icmp_sweep` anomaly in a DoS sensor to protect against address sweeps.

There are a number of IPS signatures to detect the use of ICMP probes that can gather information about your network. These signatures include `AddressMask`, `Traceroute`, `ICMP.Invalid.Packet.Size`, and `ICMP.Oversized.Packet`. Include ICMP protocol signatures in your IPS sensors to protect against these probes/attacks.

Port scans

Potential attackers may run a port scan on one or more of your hosts. This involves trying to establish a communication session to each port on a host. If the connection is successful, a service may be available that the attacker can exploit.

Use the DoS sensor anomaly `tcp_port_scan` to limit the number of sessions (complete and incomplete) from a single source IP address to the configured threshold. If the number of sessions exceed the threshold, the configured action is taken.

Use the DoS sensor anomaly `udp_scan` to limit UDP sessions in the same way.

Probes using IP traffic options

Every TCP packet has space reserved for eight flags or control bits. They are used for communicating various control messages. Although space in the packet is reserved for all eight, there are various combinations of flags that should never happen in normal network operation. For example, the SYN flag, used to initiate a session, and the FIN flag, used to end a session, should never be set in the same packet.

Attackers may create packets with these invalid combinations to test how a host will react. Various operating systems and hardware react in different ways, giving a potential attackers clues about the components of your network.

The IPS signature `TCP.Bad.Flags` detects these invalid combinations. The default action is pass though you can override the default and set it to *Block* in your IPS sensor.

Configure packet replay and TCP sequence checking

The anti-replay CLI command allows you to set the level of checking for packet replay and TCP sequence checking (or TCP Sequence (SYN) number checking). All TCP packets contain a Sequence Number (SYN) and an Acknowledgement Number (ACK). The TCP protocol uses these numbers for error free end-to-end communications. TCP sequence checking can also be used to validate individual packets.

FortiGate units use TCP sequence checking to make sure that a packet is part of a TCP session. By default, if a packet is received with sequence numbers that fall out of the expected range, the FortiGate unit drops the packet. This is normally a desired behavior, since it means that the packet is invalid. But in some cases you may want to configure different levels of anti-replay checking if some of your network equipment uses non-RFC methods when sending packets.

Configure the anti-replay CLI command:

```
config system global
    set anti-replay {disable | loose | strict}
end
```

You can set anti-replay protection to the following settings:

- **disable** — No anti-replay protection.
- **loose** — Perform packet sequence checking and ICMP anti-replay checking with the following criteria:
 - The SYN, FIN, and RST bit can not appear in the same packet.
 - The FortiGate unit does not allow more than one ICMP error packet through before it receives a normal TCP or UDP packet.
 - If the FortiGate unit receives an RST packet, and check-reset-range is set to strict, the FortiGate unit checks to determine if its sequence number in the RST is within the un-ACKed data and drops the packet if the sequence number is incorrect.
- **strict** — Performs all of the loose checking but for each new session also checks to determine if the TCP sequence number in a SYN packet has been calculated correctly and started from the correct value for each new session. Strict anti-replay checking can also help prevent SYN flooding.

If any packet fails a check it is dropped.

Configure ICMP error message verification

```
check-reset-range {disable | strict}
```

Enable ICMP error message verification to ensure an attacker can not send an invalid ICMP error message.

```
config system global
    check-reset-range {disable | strict}
end
```

- **disable** — the FortiGate unit does not validate ICMP error messages.
- **strict** — enable ICMP error message checking.

If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) | TCP(C,D) header, then if FortiOS can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. Strict checking also affects how the anti-replay option checks packets.

Protocol header checking

Select the level of checking performed on protocol headers.

```
config system global
    check-protocol-header {loose | strict}
end
```

- `loose` — the FortiGate unit performs basic header checking to verify that a packet is part of a session and should be processed. Basic header checking includes verifying that the layer-4 protocol header length, the IP header length, the IP version, the IP checksum, IP options are correct, etc.
- `strict` — the FortiGate unit does the same checking as above plus it verifies that ESP packets have the correct sequence number, SPI, and data length.

If the packet fails header checking it is dropped by the FortiGate unit.

Evasion techniques

Attackers employ a wide range of tactics to try to disguise their techniques. If an attacker disguises a known attack in such a way that it is not recognized, the attack will evade your security and possibly succeed. FortiGate security recognizes a wide variety of evasion techniques and normalizes data traffic before inspecting it.

Packet fragmentation

Information sent across local networks and the Internet is encapsulated in packets. There is a maximum allowable size for packets and this maximum size varies depending on network configuration and equipment limitations. If a packet arrives at a switch or gateway and it is too large, the data it carries is divided among two or more smaller packets before being forwarded. This is called fragmentation.

When fragmented packets arrive at their destination, they are reassembled and read. If the fragments do not arrive together, they must be held until all of the fragments arrive. Reassembly of a packet requires all of the fragments.

The FortiGate unit automatically reassembles fragmented packets before processing them because fragmented packets can evade security measures. Both IP packets and TCP packets are reassembled by the IPS engine before examination.

For example, you have configured the FortiGate unit to block access to the example.org web site. Any checks for example.com will fail if a fragmented packet arrives and one fragment contains `http://www.exa` while the other contains `mple.com/`. Viruses and malware can be fragmented and avoid detection in the same way. The FortiGate unit will reassemble fragmented packets before examining network data to ensure that inadvertent or deliberate packet fragmentation does not hide threats in network traffic.

Non-standard ports

Most traffic is sent on a standard port based on the traffic type. The FortiGate unit recognizes most traffic by packet content rather than the TCP/UDP port and uses the proper IPS signatures to examine it. Protocols recognized regardless of port include DHCP, DNP3, FTP, HTTP, IMAP, MS RPC, NNTP, POP3, RSTP, SIP, SMTP, and SSL, as well as the supported IM/P2P application protocols.

In this way, the FortiGate unit will recognize HTTP traffic being sent on port 25 as HTTP rather than SMTP, for example. Because the protocol is correctly identified, the FortiGate unit will examine the traffic for any enabled HTTP signatures.

Negotiation codes

Telnet and FTP servers and clients support the use of negotiation information to allow the server to report what features it supports. This information has been used to exploit vulnerable servers. To avoid this problem, the FortiGate unit removes negotiation codes before IPS inspection.

HTTP URL obfuscation

Attackers encode HTML links using various formats to evade detection and bypass security measures. For example, the URL `www.example.com/cgi.bin` could be encoded in a number of ways to avoid detection but still work properly, and be interpreted the same, in a web browser.

The FortiGate prevents the obfuscation by converting the URL to ASCII before inspection.

Table 1: HTTP URL obfuscation types

Encoding type	Example
No encoding	<code>http://www.example.com/cgi.bin/</code>
Decimal encoding	<code>http://www.example.com/&#99;&#103;&#105;&#46;&#98;&#105;&#110;&#47;</code>
URL encoding	<code>http://www.example.com/%43%47%49%2E%42%49%4E%2F</code>
ANSI encoding	<code>http://www.example.com/%u0063%u0067%u0069%u002E%u0062%u0069%u006E/</code>
Directory traversal	<code>http://www.example.com/cgi.bin/test/..</code>

HTTP header obfuscation

The headers of HTTP requests or responses can be modified to make the discovery of patterns and attacks more difficult. To prevent this, the FortiGate unit will:

- remove junk header lines
- reassemble an HTTP header that's been folded onto multiple lines
- move request parameters to HTTP POST body from the URL

The message is scanned for any enabled HTTP IPS signatures once these problems are corrected.

HTTP body obfuscation

The body content of HTTP traffic can be hidden in an attempt to circumvent security scanning. HTTP content can be GZipped or deflated to prevent security inspection. The FortiGate unit will uncompress the traffic before inspecting it.

Another way to hide the contents of HTTP traffic is to send the HTTP body in small pieces, splitting signature matches across two separate pieces of the HTTP body. The FortiGate unit reassembles these 'chunked bodies' before inspection.

Microsoft RPC evasion

Because of its complexity, the Microsoft Remote Procedure Call protocol suite is subject to a number of known evasion techniques, including:

- SMB-level fragmentation
- DCERPC-level fragmentation
- DCERPC multi-part fragmentation
- DCERPC UDP fragmentation
- Multiple DCERPC fragments in one packet

The FortiGate unit reassembles the fragments into their original form before inspection.

Defending against DoS attacks

A denial of service is the result of an attacker sending an abnormally large amount of network traffic to a target system. Having to deal with the traffic flood slows down or disables the target system so that legitimate users can not use it for the duration of the attack.

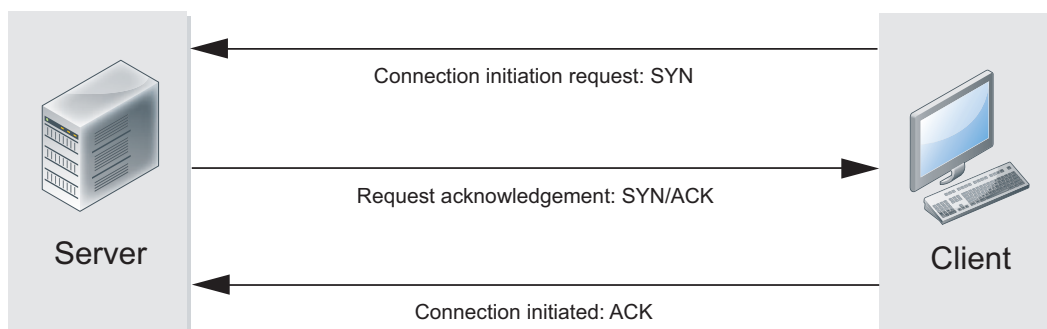
Any network traffic the target system receives has to be examined, and then accepted or rejected. TCP, UDP, and ICMP traffic is most commonly used, but a particular type of TCP traffic is the most effective. TCP packets with the SYN flag are the most efficient DoS attack tool because of how communication sessions are started between systems.

The “three-way handshake”

Communication sessions between systems start with establishing a TCP/IP connection. This is a simple three step process, sometimes called a “three-way handshake,” initiated by the client attempting to open the connection.

- 1 The client sends a TCP packet with the SYN flag set. With the SYN packet, the client informs the server of its intention to establish a connection.
- 2 If the server is able to accept the connection to the client, it sends a packet with the SYN and the ACK flags set. This simultaneously acknowledges the SYN packet the server has received, and informs the client that the server intends to establish a connection.
- 3 To acknowledge receipt of the packet and establish the connection, the client sends an ACK packet.

Figure 1: Establishing a TCP/IP connection



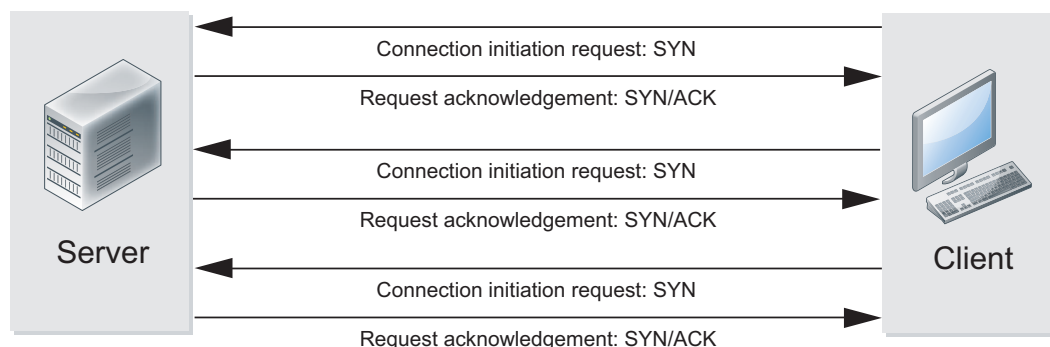
The three-way handshake is a simple way for the server and client to each agree to establish a connection and acknowledge the other party expressing its intent. Unfortunately, the three-way handshake can be used to interfere with communication rather than facilitate it.

SYN flood

When a client sends a SYN packet to a server, the server creates an entry in its session table to keep track of the connection. The server then sends a SYN+ACK packet expecting an ACK reply and the establishment of a connection.

An attacker intending to disrupt a server with a denial of service (DoS) attack can send a flood of SYN packets and not respond to the SYN+ACK packets the server sends in response. Networks can be slow and packets can get lost so the server will continue to send SYN+ACK packets until it gives up, and removes the failed session from the session table. If an attacker sends enough SYN packets to the server, the session table will fill completely, and further connection attempts will be denied until the incomplete sessions time out. Until this happens, the server is unavailable to service legitimate connection requests.

Figure 2: A single client launches a SYN flood attack

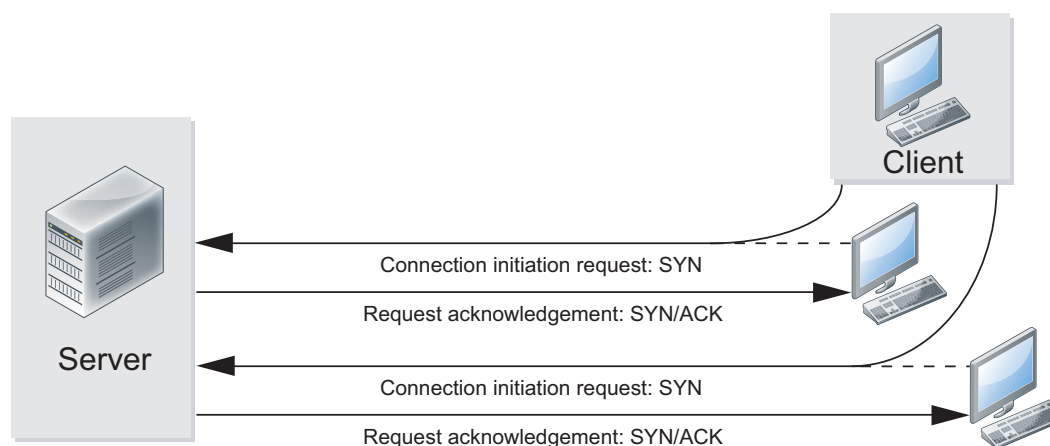


SYN floods are seldom launched from a single address so limiting the number of connection attempts from a single IP address is not usually effective.

SYN spoofing

With a flood of SYN packets coming from a single attacker, you can limit the number of connection attempts from the source IP address or block the attacker entirely. To prevent this simple defense from working, or to disguise the source of the attack, the attacker may spoof the source address and use a number of IP addresses to give the appearance of a distributed denial of service (DDoS) attack. When the server receives the spoofed SYN packets, the SYN+ACK replies will go to the spoofed source IP addresses which will either be invalid, or the system receiving the reply will not know what to do with it.

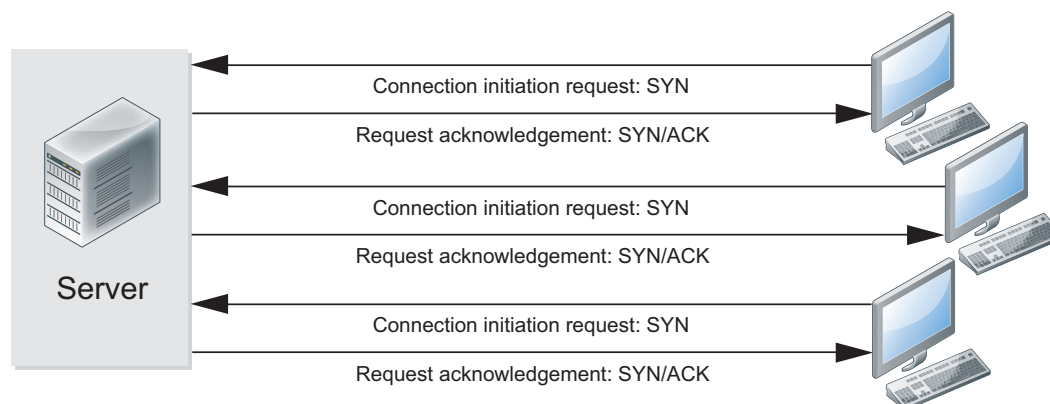
Figure 3: A client launches a SYN spoof attack



DDoS SYN flood

The most severe form of SYN attack is the distributed SYN flood, one variety of distributed denial of service attack (DDoS). Like the SYN flood, the target receives a flood of SYN packets and the ACK+SYN replies are never answered. The attack is distributed across multiple sources sending SYN packets in a coordinated attack.

Figure 4: Multiple attackers launch a distributed SYN flood



The distributed SYN flood is more difficult to defend against because multiple clients are capable of creating a larger volume of SYN packets than a single client. Even if the server can cope, the volume of traffic may overwhelm a point in the network upstream of the targeted server. The only defence against this is more bandwidth to prevent any choke-points.

Configuring the SYN threshold to prevent SYN floods

The preferred primary defence against any type of SYN flood is the DoS sensor `tcp_syn_flood` threshold. The threshold value sets an upper limit on the number of new incomplete TCP connections allowed per second. If the number of incomplete connections exceeds the threshold value, and the action is set to *Pass*, the FortiGate unit will allow the SYN packets that exceed the threshold. If the action is set to *Block*, the FortiGate unit will block the SYN packets that exceed the threshold, but it will allow SYN packets from clients that send another SYN packet.

The tools attackers use to generate network traffic will not send a second SYN packet when a SYN+ACK response is not received from the server. These tools will not “retry.” Legitimate clients will retry when no response is received, and these retries are allowed even if they exceed the threshold with the action set to *Block*.

For more information, see [“Creating and configuring a DoS sensor” on page 218](#). For recommendations on how to configure DoS policies, see [“DoS policy recommendations” on page 28](#).

SYN proxy

FortiGate units with network acceleration hardware, whether built-in or installed in the form of an add-on module, offer a third action for the `tcp_syn_flood` threshold. Instead of *Block* and *Pass*, you can choose to *Proxy* the incomplete connections that exceed the threshold value.

When the `tcp_syn_flood` threshold action is set to *Proxy*, incomplete TCP connections are allowed as normal as long as the configured threshold is not exceeded. If the threshold is exceeded, the FortiGate unit will intercept incoming SYN packets from clients and respond with a SYN+ACK packet. If the FortiGate unit receives an ACK response as expected, it will “replay” this exchange to the server to establish a communication session between the client and the server, and allow the communication to proceed.

Other flood types

UDP and ICMP packets can also be used for DoS attacks, though they are less common. TCP SYN packets are so effective because the target receives them and maintains a session table entry for each until they time out. Attacks using UDP or ICMP packets do not require the same level of attention from a target, rendering them less effective. The target will usually drop the offending packets immediately, closing the session.

Use the `udp_flood` and `icmp_flood` thresholds to defend against these DoS attacks.

Traffic inspection

When the FortiGate unit examines network traffic one packet at a time for IPS signatures, it is performing traffic analysis. This is unlike content analysis where the traffic is buffered until files, email messages, web pages, and other files are assembled and examined as a whole.

DoS policies use traffic analysis by keeping track of the type and quantity of packets, as well as their source and destination addresses.

Application control uses traffic analysis to determine which application generated the packet.

Although traffic inspection doesn't involve taking packets and assembling files they are carrying, the packets themselves can be split into fragments as they pass from network to network. These fragments are reassembled by the FortiGate unit before examination.

No two networks are the same and few recommendations apply to all networks. This topic offers suggestions on how you can use the FortiGate unit to help secure your network against content threats.

IPS signatures

IPS signatures can detect malicious network traffic. For example, the Code Red worm attacked a vulnerability in the Microsoft IIS web server. Your FortiGate's IPS system can detect traffic attempting to exploit this vulnerability. IPS may also detect when infected systems communicate with servers to receive instructions.

IPS recommendations

- Enable IPS scanning at the network edge for all services.
- Use FortiClient endpoint IPS scanning for protection against threats that get into your network.
- Subscribe to FortiGuard IPS Updates and configure your FortiGate unit to receive push updates. This will ensure you receive new IPS signatures as soon as they are available.

- Your FortiGate unit includes IPS signatures written to protect specific software titles from DoS attacks. Enable the signatures for the software you have installed and set the signature action to *Block*.

You can view these signatures by going to *UTM Profiles > Intrusion Protection > Predefined* and sorting by, or applying a filter to, the *Group* column.

- Because it is critical to guard against attacks on services that you make available to the public, configure IPS signatures to block matching signatures. For example, if you have a web server, configure the action of web server signatures to *Block*.

Suspicious traffic attributes

Network traffic itself can be used as an attack vector or a means to probe a network before an attack. For example, SYN and FIN flags should never appear together in the same TCP packet. The SYN flag is used to initiate a TCP session while the FIN flag indicates the end of data transmission at the end of a TCP session.

The FortiGate unit has IPS signatures that recognize abnormal and suspicious traffic attributes. The SYN/FIN combination is one of the suspicious flag combinations detected in TCP traffic by the `TCP.BAD.FLAGS` signature.

The signatures that are created specifically to examine traffic options and settings, begin with the name of the traffic type they are associated with. For example, signatures created to examine TCP traffic have signature names starting with TCP.

DoS policies

DDoS attacks vary in nature and intensity. Attacks aimed at saturating the available bandwidth upstream of your service can only be countered by adding more bandwidth. DoS policies can help protect against DDoS attacks that aim to overwhelm your server resources.

DoS policy recommendations

- Use and configure DoS policies to appropriate levels based on your network traffic and topology. This will help drop traffic if an abnormal amount is received.
- It is important to set a good threshold. The threshold defines the maximum number of sessions/packets per second of normal traffic. If the threshold is exceeded, the action is triggered. Threshold defaults are general recommendations, although your network may require very different values.

One way to find the correct values for your environment is to set the action to *Pass* and enable logging. Observe the logs and adjust the threshold values until you can determine the value at which normal traffic begins to generate attack reports. Set the threshold above this value with the margin you want. Note that the smaller the margin, the more protected your system will be from DoS attacks, but your system will also be more likely to generate false alarms.

Application control

While applications can often be blocked by the ports they use, application control allows convenient management of all supported applications, including those that do not use set ports.

Application control recommendations

- Some applications behave in an unusual manner in regards to application control. For more information, see [“Application considerations” on page 207](#).

- By default, application control allows the applications not specified in the application control list. For high security networks, you may want to change this behavior so that only the explicitly allowed applications are permitted.

Content inspection and filtering

When the FortiGate unit buffers the packets containing files, email messages, web pages, and other similar files for reassembly before examining them, it is performing content inspection. Traffic inspection, on the other hand, is accomplished by the FortiGate unit examining individual packets of network traffic as they are received.

No two networks are the same and few recommendations apply to all networks. This topic offers suggestions on how you can use the FortiGate unit to help secure your network against content threats. Be sure to understand the effects of the changes before using the suggestions.

AntiVirus

The FortiGate antivirus scanner can detect viruses and other malicious payloads used to infect machines. The FortiGate unit performs deep content inspection. To prevent attempts to disguise viruses, the antivirus scanner will reassemble fragmented files and uncompress content that has been compressed. Patented Compact Pattern Recognition Language (CPRL) allows further inspection for common patterns, increasing detection rates of virus variations in the future.

AntiVirus recommendations

- Enable antivirus scanning at the network edge for all services.
- Use FortiClient endpoint antivirus scanning for protection against threats that get into your network.
- Subscribe to FortiGuard AntiVirus Updates and configure your FortiGate unit to receive push updates. This will ensure you receive new antivirus signatures as soon as they are available.
- Enable the Extended Virus Database if your FortiGate unit supports it.
- Examine antivirus logs periodically. Take particular notice of repeated detections. For example, repeated virus detection in SMTP traffic could indicate a system on your network is infected and is attempting to contact other systems to spread the infection using a mass mailer.
- The *builtin-patterns* file filter list contains nearly 20 file patterns. Many of the represented files can be executed or opened with a double-click. If any of these file patterns are not received as a part of your normal traffic, blocking them may help protect your network. This also saves resources since files blocked in this way do not need to be scanned for viruses.
- To conserve system resources, avoid scanning email messages twice. Scan messages as they enter and leave your network or when clients send and retrieve them, rather than both.

FortiGuard Web Filtering

The web is the most popular part of the Internet and, as a consequence, virtually every computer connected to the Internet is able to communicate using port 80, HTTP. Botnet communications take advantage of this open port and use it to communicate with infected computers. FortiGuard Web Filtering can help stop infections from malware sites and help prevent communication if an infection occurs.

FortiGuard Web Filtering recommendations

- Enable FortiGuard Web Filtering at the network edge.
- Install the FortiClient application and use FortiGuard Web Filtering on any systems that bypass your FortiGate unit.
- Block categories such as Pornography, Malware, Spyware, and Phishing. These categories are more likely to be dangerous.
- In the email filter profile, enable *IP Address Check* in *FortiGuard Email Filtering*. Many IP addresses used in spam messages lead to malicious sites; checking them will protect your users and your network.

Email filter

Spam is a common means by which attacks are delivered. Users often open email attachments they should not, and infect their own machine. The FortiGate email filter can detect harmful spam and mark it, alerting the user to the potential danger.

Email filter recommendations

- Enable email filtering at the network edge for all types of email traffic.
- Use FortiClient endpoint scanning for protection against threats that get into your network.
- Subscribe to the FortiGuard AntiSpam Service.

DLP

Most security features on the FortiGate unit are designed to keep unwanted traffic out of your network while DLP can help you keep sensitive information from leaving your network. For example, credit card numbers and social security numbers can be detected by DLP sensors.

DLP recommendations

- Rules related to HTTP posts can be created, but if the requirement is to block all HTTP posts, a better solution is to use application control or the *HTTP POST Action* option in the web filter profile.
- While DLP can detect sensitive data, it is more efficient to block unnecessary communication channels than to use DLP to examine it. If you don't use instant messaging or peer-to-peer communication in your organization, for example, use application control to block them entirely.



AntiVirus

This section describes how to configure the antivirus options. From an antivirus profile you can configure the FortiGate unit to apply antivirus protection to HTTP, FTP, IMAP, POP3, SMTP, IM, and NNTP sessions. If your FortiGate unit supports SSL content scanning and inspection, you can also configure antivirus protection for HTTPS, IMAPS, POP3S, SMTPS, and FTPS sessions.

The following topics are included in this section:

- [Antivirus concepts](#)
- [Enable antivirus scanning](#)
- [Enable the file quarantine](#)
- [Enable grayware scanning](#)
- [Testing your antivirus configuration](#)
- [Antivirus examples](#)

Antivirus concepts

The word “antivirus” refers to a group of features that are designed to prevent unwanted and potentially malicious files from entering your network. These features all work in different ways, which include checking for a file size, name, or type, or for the presence of a virus or grayware signature.

The antivirus scanning routines your FortiGate unit uses are designed to share access to the network traffic. This way, each individual feature does not have to examine the network traffic as a separate operation, and the overhead is reduced significantly. For example, if you enable file filtering and virus scanning, the resources used to complete these tasks are only slightly greater than enabling virus scanning alone. Two features do not require twice the resources.

How antivirus scanning works

Antivirus scanning examines files for viruses, worms, trojans, and malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action.

The most thorough scan requires that the FortiGate unit have the whole file for the scanning procedure. To achieve this, the antivirus proxy buffers the file as it arrives. Once the transmission is complete, the virus scanner examines the file. If no infection is present, it is sent to the destination. If an infection is present, a replacement message is set to the destination.

During the buffering and scanning procedure, the client must wait. With a default configuration, the file is released to the client only after it is scanned. You can enable client comforting in the protocol options profile to feed the client a trickle of data to prevent them from thinking the transfer is stalled, and possibly cancelling the download.

Buffering the entire file allows the FortiGate unit to eliminate the danger of missing an infection due to fragmentation because the file is reassembled before examination. Archives can also be expanded and the contents scanned, even if archives are nested.

Since the FortiGate unit has a limited amount of memory, files larger than a certain size do not fit within the memory buffer. The default buffer size is 10 MB. You can use the `uncompsizelimit` CLI command to adjust the size of this memory buffer.

Files larger than the buffer are passed to the destination without scanning. You can use the *Oversize File/Email* setting to block files larger than the antivirus buffer if allowing files that are too large to be scanned is an unacceptable security risk.

Flow-based antivirus scanning

If your FortiGate unit supports flow-based antivirus scanning, you can choose to select it instead of proxy-based antivirus scanning. Flow-based antivirus scanning uses the FortiGate IPS engine to examine network traffic for viruses, worms, trojans, and malware, without the need to buffer the file being checked.

The advantages of flow-based scanning include faster scanning and no maximum file size. Flow-based scanning doesn't require the file be buffered so it is scanned as it passes through the FortiGate unit, packet-by-packet. This eliminates the maximum file size limit and the client begins receiving the file data immediately.

The trade-off for these advantages is that flow-based scans detect a smaller number of infections. Viruses in documents, packed files, and some archives are less likely to be detected because the scanner can only examine a small portion of the file at any moment. Also, the file archive formats flow-based scanning will examine are limited to ZIP and GZIP.

Antivirus scanning order

The antivirus scanning function includes various modules and engines that perform separate tasks.

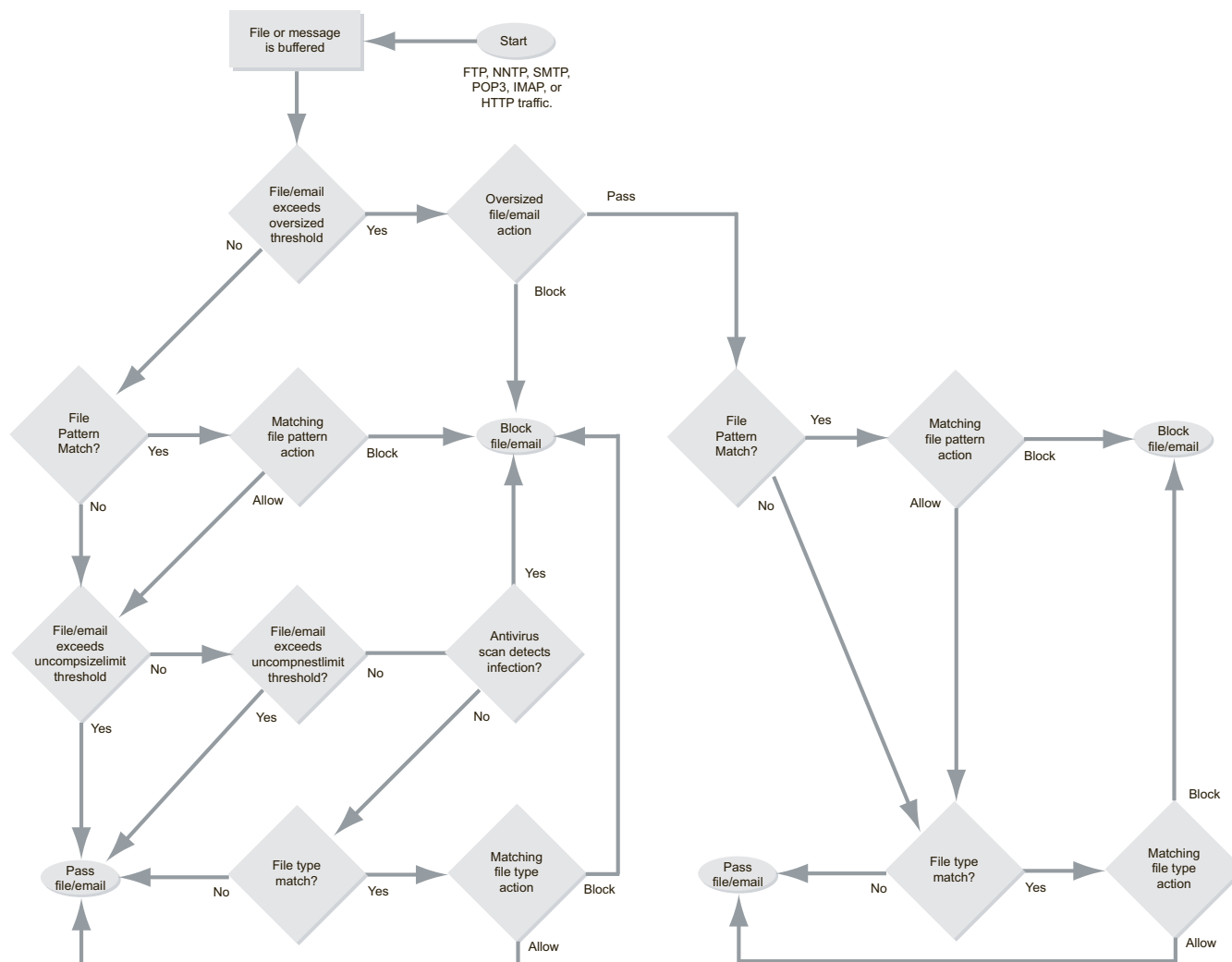
Proxy-based antivirus scanning order

Figure 5 on page 33 illustrates the antivirus scanning order when using proxy-based scanning (i.e. the normal, extended, or extreme databases). The first check for oversized files/email is to determine whether the file exceeds the configured size threshold. The `uncompsizelimit` check is to determine if the file can be buffered for file type and antivirus scanning. If the file is too large for the buffer, it is allowed to pass without being scanned. For more information, see the `config antivirus service` command in the [FortiGate CLI Reference](#). The antivirus scan includes scanning for viruses, as well as for grayware and heuristics if they are enabled.



File filtering includes file pattern and file type scans which are applied at different stages in the antivirus process.

Figure 5: Antivirus scanning order when using the normal, extended, or extreme database



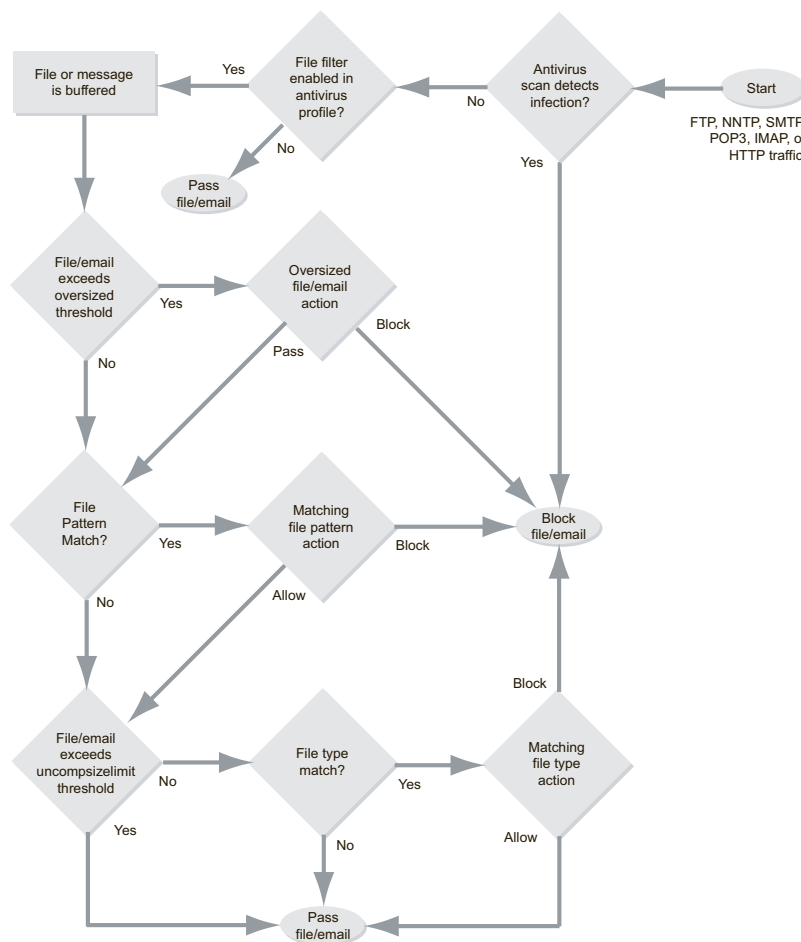
If a file fails any of the tasks of the antivirus scan, no further scans are performed. For example, if the file `fakefile.EXE` is recognized as a blocked file pattern, the FortiGate unit will send the end user a replacement message, and delete or quarantine the file. The unit will not perform virus scan, grayware, heuristics, and file type scans because the previous checks have already determined that the file is a threat and have dealt with it.

Flow-based antivirus scanning order

Figure 6 on page 34 illustrates the antivirus scanning order when using flow-based scanning (i.e. the flow-based database). The antivirus scan takes place before any other antivirus-related scan. If file filter is not enabled, the file is not buffered. The antivirus scan includes scanning for viruses, as well as for grayware and heuristics if they are enabled.



File filtering includes file pattern and file type scans which are applied at different stages in the antivirus process.

Figure 6: Antivirus scanning order when using the flow-based database

Antivirus databases

The antivirus scanning engine relies on a database to detail the unique attributes of each infection. The antivirus scan searches for these signatures, and when one is discovered, the FortiGate unit determines the file is infected and takes action.

All FortiGate units have the normal antivirus signature database but some models have additional databases you can select for use. Which you choose depends on your network and security needs.

Normal	Includes viruses currently spreading as determined by the FortiGuard Global Security Research Team. These viruses are the greatest threat. The Normal database is the default selection and it is available on every FortiGate unit.
Extended	Includes the normal database in addition to recent viruses that are no-longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared.

Extreme	Includes the extended database in addition to a large collection of 'zoo' viruses. These are viruses that have not spread in a long time and are largely dormant today. Some zoo viruses may rely on operating systems and hardware that are no longer widely used.
Flow	The flow-based database is a subset of the extreme database. Flow-based scans can not detect polymorphic and packed-file viruses so those signatures are not included in the flow-based database. Note that flow-based scanning is not just another database, but a different type of scanning. For more information, see "How antivirus scanning works" on page 31 .

Antivirus techniques

The antivirus features work in sequence to efficiently scan incoming files and offer your network optimum antivirus protection. The first four features have specific functions, the fifth, heuristics, protects against any new, previously unknown virus threats. To ensure that your system is providing the most protection available, all virus definitions and signatures are updated regularly through the FortiGuard antivirus services. The features are discussed in the order that they are applied, followed by FortiGuard antivirus.

Virus scan

If the file passes the file pattern scan, the FortiGate unit applies a virus scan to it. The virus definitions are kept up-to-date through the FortiGuard Distribution Network (FDN). For more information, see ["FortiGuard Antivirus" on page 35](#).

Grayware

If the file passes the virus scan, it will be checked for grayware. Grayware configurations can be turned on and off as required and are kept up to date in the same manner as the antivirus definitions. For more information, see ["Enable grayware scanning" on page 42](#).

Heuristics

After an incoming file has passed the grayware scan, it is subjected to the heuristics scan. The FortiGate heuristic antivirus engine, if enabled, performs tests on the file to detect virus-like behavior or known virus indicators. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results.



You can configure heuristics only through the CLI. See the [FortiGate CLI Reference](#).

FortiGuard Antivirus

FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The [FortiGuard Center](#) web site also provides the FortiGuard Antivirus virus and attack encyclopedia.

The connection between the FortiGate unit and FortiGuard Center is configured in *System > Maintenance > FortiGuard*.

Enable antivirus scanning

Antivirus scanning is enabled in the antivirus profile. Once the antivirus profile is enabled and selected in one or more firewall policies, all the traffic controlled by those firewall policies will be scanned according to your settings.

To enable antivirus scanning — web-based manager

- 1 Go to *UTM Profiles > AntiVirus > Profile*.
- 2 Select *Create New* to create a new antivirus profile, or select an existing antivirus profile and choose *Edit*.
- 3 In the row labeled *Virus Scan and Removal*, select the check boxes associated with the traffic you want scanned for viruses.
- 4 Select *OK*.

To enable antivirus scanning — CLI

You need to configure the scan option for each type of traffic you want scanned. In this example, antivirus scanning of HTTP traffic is enabled in the profile.

```
config antivirus profile
  edit my_av_profile
    config http
      set options scan
    end
  end
```

Viewing antivirus database information

The FortiGate antivirus scanner relies on up-to-date virus signatures to detect the newest threats. To view the information about the FortiGate unit virus signatures, check the status page or the *Virus Database* information page:

- **Status page:** Go to *System > Dashboard > Dashboard*. In the *License Information* section under *FortiGuard Services*, the *AV Definitions* field shows the regular antivirus database version as well as when it was last updated.

If your FortiGate unit supports extended and extreme virus database definitions, the database versions and date they were last updated is displayed in the *Extended set* and *Extreme DB* fields.

The flow-based virus database is distributed as part of the IPS signature database. Its database version and date it was last updated is displayed in the *IPS Definitions* field.

- **Virus Database:** Go to *UTM Profiles > AntiVirus > Virus Database*. This page shows the version number, number of included signatures, and a description of the regular virus database.

If your FortiGate unit supports extended, extreme, or flow-based virus database definitions, the version numbers, number of included signatures, and descriptions of those databases are also displayed.

Changing the default antivirus database

If your FortiGate unit supports extended, extreme, or flow-based virus database definitions, you can select the virus database most suited to your needs.

In most circumstances, the regular virus database provides sufficient protection. Viruses known to be active are included in the regular virus database. The extended database includes signatures of the viruses that have become rare within the last year in addition to those in the normal database. The extreme database includes legacy viruses that have not been seen in the wild in a long time in addition to those in the extended database.

The flow-based database contains a subset of the virus signatures in the extreme database. Unlike the other databases, selecting the flow-based database also changes the way the FortiGate unit scans your network traffic for viruses. Instead of the standard proxy-based scan, network traffic is scanned as it streams through the FortiGate unit. For more information on the differences between flow-based and proxy-based antivirus scanning, see [“How antivirus scanning works” on page 31](#).

If you require the most comprehensive antivirus protection, enable the extended virus database. The additional coverage comes at a cost, however, because the extra processing requires additional resources.

To change the antivirus database — web-based manager

- 1 Go to *UTM Profiles > AntiVirus > Virus Database*.
- 2 Select the antivirus database the FortiGate unit will use as the default database to perform antivirus scanning of your network traffic.
- 3 Select *Apply*.

To change the antivirus database — CLI

```
config antivirus settings
  set default-db extended
end
```

Overriding the default antivirus database

The default antivirus database is used for all antivirus scanning. If you have a particular policy or traffic type that requires scanning using a different antivirus database, you can override the default database. Antivirus database overrides are applied to individual traffic types in an antivirus profile. The override will affect only the traffic types to which the override is applied for the traffic handled by the security policy the antivirus profile is applied to. Antivirus database overrides can be set using only the CLI.

In this example, a database override is applied to HTTP traffic in a protocol options profile named `web_traffic`. The flow-based database is specified.

To override the default antivirus database — CLI

```
config antivirus profile
  edit web-traffic
    config http
      set avdb flow-based
    end
  end
```

With this configuration, the flow-based database is used for antivirus scans on HTTP traffic controlled by firewall policies in which this antivirus profile is selected. Other traffic types will use the default database, as specified in *UTM Profiles > AntiVirus > Virus Database*.

Adding the antivirus profile to a security policy

This procedure is required only if your antivirus profile does not yet belong to a security policy. You need to add the antivirus profile to a policy before any antivirus profile settings can take effect.

To add the antivirus profile to a policy

- 1 Go to *Policy > Policy > Policy*.
- 2 Select *Create New* to add a new policy, or select the *Edit* icon of the security policy to which you want to add the profile.
- 3 Enable *UTM*.
- 4 Select *Enable AntiVirus* and select the antivirus profile that contains the quarantine configuration.
- 5 Select *OK* to save the security policy.

Configuring the scan buffer size

When checking files for viruses using the proxy-based scanning method, there is a maximum file size that can be buffered. Files larger than this size are passed without scanning. The default size for all FortiGate models is 10 megabytes.

Archived files are extracted and email attachments are decoded before the FortiGate unit determines if they can fit in the scan buffer. For example, a 7 megabyte ZIP file containing a 12 megabyte EXE file will be passed without scanning with the default buffer size. Although the archive would fit within the buffer, the uncompressed file size will not.

In this example, the `uncompsizelimit` CLI command is used to change the scan buffer size to 20 megabytes for files found in HTTP traffic:

```
config antivirus service http
  set uncompsizelimit 20
end
```

The maximum buffer size varies by model. Enter `set uncompsizelimit ?` to display the buffer size range for your FortiGate unit.



Flow-based scanning does not use a buffer and therefore has no file-size limit. File data is scanned as it passes through the FortiGate unit. The `uncompsizelimit` setting has no effect for flow-based scanning.

Configuring archive scan depth

The antivirus scanner will open archives and scan the files inside. Archives within other archives, or nested archives, are also scanned to a default depth of twelve nestings. You can adjust the number of nested archives to which the FortiGate unit will scan with the `uncompnestlimit` CLI command. Further, the limit is configured separately for each traffic type.

For example, this CLI command sets the archive scan depth for SMTP traffic to 5. That is, archives within archives will be scanned five levels deep.

```
config antivirus service smtp
  set uncompnestlimit 5
end
```

You can set the nesting limit from 2 to 100.

Configuring a maximum allowed file size

The protocol option profile allows you to enforce a maximum allowed file size for each of the network protocols in the profile. They are HTTP, FTP, IMAP, POP3, SMTP, IM, and NNTP. If your FortiGate unit supports SSL content scanning and inspection, you can also configure a maximum file size for HTTPS, IMAPS, POP3S, SMTPS, and FTPS.

The action you set determines what the FortiGate unit does with a file that exceeds the oversized file threshold. Two actions are available:

Block	Files that exceed the oversize threshold are dropped and a replacement message is sent to the user instead of the file.
Pass	Files exceed the oversized threshold are allowed through the FortiGate unit to their destination. Note that passed files are not scanned for viruses. File Filtering, both file pattern and file type, are applied, however.

You can also use the maximum file size to help secure your network. If you're using a proxy-based virus scan, the proxy scan buffer size limits the size of the files that can be scanned for infection. Files larger than this limit are passed without scanning. If you configure the maximum file size to block files larger than the scan buffer size, large infected files will not by-pass antivirus scanning.

In this example, the maximum file size will be configured to block files larger than 10 megabytes, the largest file that can be antivirus scanned with the default settings. You will need to configure a protocol options profile and add it to a security policy.

Create a protocol options profile to block files larger than 10 MB

- 1 Go to *Policy > Policy > Protocol Options*.
- 2 Select *Create New*.
- 3 Enter `10MB_Block` for the protocol options policy name.
- 4 For the comment, enter `Files larger than 10MB are blocked`.
- 5 Expand each protocol listed and select *Block* for the *Oversized File/Email* setting. Also confirm that the *Threshold* is set to 10.
- 6 Select *OK*.

The protocol options profile is configured, but to block files, you must select it in the firewall profiles handling the traffic that contains the files you want blocked.

To select the protocol options profile in a security policy

- 1 Go to *Policy > Policy > Policy*.
- 2 Select a security policy.
- 3 Select the *Edit* icon.
- 4 Enable *UTM*.
- 5 Select `10MB_Block` from the *Protocol Options* list.
- 6 Select *OK* to save the security policy.

Once you complete these steps, any files in the traffic handled by this policy that are larger than 10MB will be blocked. If you have multiple firewall policies, examine each to determine if you want to apply similar file blocking the them as well.

Configuring client comforting

When proxy-based antivirus scanning is enabled, the FortiGate unit buffers files as they are downloaded. Once the entire file is captured, the FortiGate unit scans it. If no infection is found, the file is sent along to the client. The client initiates the file transfer and nothing happens until the FortiGate finds the file clean, and releases it. Users can be impatient, and if the file is large or the download slow, they may cancel the download, not realizing that the transfer is in progress.

The client comforting feature solves this problem by allowing a trickle of data to flow to the client so they can see the file is being transferred. The default client comforting transfer rate sends one byte of data to the client every ten seconds. This slow transfer continues while the FortiGate unit buffers the file and scans it. If the file is infection-free, it is released and the client will receive the remainder of the transfer at full speed. If the file is infected, the FortiGate unit caches the URL and drops the connection. The client does not receive any notification of what happened because the download to the client had already started. Instead, the download stops and the user is left with a partially downloaded file.

If the user tries to download the same file again within a short period of time, the cached URL is matched and the download is blocked. The client receives the Infection cache message replacement message as a notification that the download has been blocked. The number of URLs in the cache is limited by the size of the cache.



Client comforting can send unscanned and therefore potentially infected content to the client. You should only enable client comforting if you are prepared to accept this risk. Keeping the client comforting interval high and the amount low will reduce the amount of potentially infected data that is downloaded.

Client comforting is available for HTTP and FTP traffic. If your FortiGate unit supports SSL content scanning and inspection, you can also configure client comforting for HTTPS and FTPS traffic.

Enable and configure client comforting

- 1 Go to *Policy > Policy > Protocol Options*.
- 2 Select a protocol options profile and choose *Edit*, or select *Create New* to make a new one.
- 3 Expand HTTP, FTP, and if your FortiGate unit supports SSL content scanning and inspection, expand HTTPS and FTPS as well.
- 4 To enable client comforting, select *Comfort Clients* for each of the protocols in which you want it enabled.
- 5 Select *OK* to save the changes.
- 6 Select this protocol options profile in any security policy for it to take effect on all traffic handled by the policy.

The default values for Interval and Amount are 10 and 1, respectively. This means that when client comforting takes effect, 1 byte of the file is sent to the client every 10 seconds. You can change these values to vary the amount and frequency of the data transferred by client comforting.

Enable the file quarantine

You can quarantine blocked and infected files if you have a FortiGate unit with a local hard disk. You can view the file name and status information about the file in the *Quarantined Files* list and submit specific files and add file patterns to the *AutoSubmit* list so they will automatically be uploaded to the FortiGuard AntiVirus service for analysis.

FortiGate units can also quarantine blocked and infected files to a FortiAnalyzer unit. Files stored on the FortiAnalyzer unit can also be viewed from the *Quarantined Files* list in the FortiGate unit.

General configuration steps

The following steps provide an overview of the file quarantine configuration. For best results, follow the procedures in the order given. Note that if you perform any additional actions between procedures, your configuration may have different results.

- 1 Go to *UTM Profiles > AntiVirus > Quarantine* to configure the quarantine service and destination.
- 2 Go to *UTM Profiles > AntiVirus > Profile* and edit an existing antivirus profile or create a new one. In the *Quarantine* row, select the check boxes of the protocols for which you want the quarantine enabled. The *Quarantine* option only appears if your FortiGate unit has a local disk or if your FortiGate unit is configured to use a FortiAnalyzer unit to quarantine files.



Antivirus profiles also have a configurable feature called *Quarantine Virus Sender (to Banned User List)*. This is a different feature unrelated to the *Quarantine* option.

- 3 If you have not previously done so, go to *Policy > Policy > Policy* and add the antivirus profile to a security policy.

Configuring the file quarantine

You can configure quarantine options for HTTP, FTP, IMAP, POP3, SMTP, IM, and NNTP Traffic. If your FortiGate unit supports SSL content scanning and inspection you can also quarantine blocked and infected files from HTTPS, IMAPS, POP3S, SMTPS, and FTPS traffic.

The quarantine configuration is only available in the CLI. See the [CLI Reference](#) for a full description of the `config antivirus quarantine` command.

In this example, the quarantine is configured to use the FortiGate unit disk, save files for 24 hours, use a maximum of 500 MB, and overwrite the oldest file with a new one should the disk space limit be exceeded.

To configure the file quarantine

```
config antivirus quarantine
  set destination disk
  set agelimit 24
  set quarantine-quota 500
  set lowspace ovrw-old
end
```

Viewing quarantined files

The *Quarantined Files* list displays information about each quarantined file. You can sort the files by file name, date, service, status, duplicate count (DC), or time to live (TTL). You can also filter the list to view only quarantined files from a specific service.

To view quarantined files, go to *Log&Report > Quarantined Files*.

Downloading quarantined files

You can download any non-expired file from the quarantine. You may want to do so if it was quarantined as the result of a false positive or if you want to examine the contents.

To download a quarantined file

- 1 Go to *Log&Report > Quarantined Files*.
- 2 In the quarantine file list, find the file you want to download.

To find the file more quickly, use the *Sort by* function to change the sort order. Available sort criteria include status, services, file name, date, TTL, and duplicate count. You can also use the *Filter* function to display the files quarantined from an individual traffic type.
- 3 Select the *Download* icon to save a copy of the quarantined file on your computer.

Enable grayware scanning

Grayware programs are unsolicited software programs installed on computers, often without the user's consent or knowledge. Grayware programs are generally considered an annoyance, but they can also cause system performance problems or be used for malicious purposes.

To allow the FortiGate unit to scan for known grayware programs, you must enable both antivirus scanning and grayware detection. By default, grayware detection is disabled. To enable antivirus scanning, see ["Enable antivirus scanning" on page 36](#).

To enable grayware detection — web-based manager

- 1 Go to *UTM Profiles > AntiVirus > Virus Database*.
- 2 Select *Enable Grayware Detection*.

To enable grayware detection — CLI

```
config antivirus settings
    set grayware enable
end
```

With grayware detection enabled, the FortiGate unit will scan for grayware any time it checks for viruses.

Testing your antivirus configuration

You have configured your FortiGate unit to stop viruses, but you'd like to confirm your settings are correct. Even if you have a real virus, it would be dangerous to use for this purpose. An incorrect configuration will allow the virus to infect your network.

To solve this problem, the European Institute of Computer Anti-virus Research has developed a test file that allows you to test your antivirus configuration. The EICAR test file is not a virus. It can not infect computers, nor can it spread or cause any damage. It's a very small file that contains a sequence of characters. Your FortiGate unit recognizes the EICAR test file as a virus so you can safely test your FortiGate unit antivirus configuration.

Go to <http://www.fortiguard.com/antivirus/eicartest.html> to download the test file (eicar.com) or the test file in a ZIP archive (eicar.zip).

If the antivirus profile applied to the security policy that allows you access to the Web is configured to scan HTTP traffic for viruses, any attempt to download the test file will be blocked. This indicates that you are protected.

Antivirus examples

The following examples provide a sample antivirus configuration scenario for a fictitious company.

Configuring simple antivirus protection

Small offices, whether they are small companies, home offices, or satellite offices, often have very simple needs. This example details how to enable antivirus protection on a FortiGate unit located in a satellite office. The satellite office does not have an internal email server. To send and retrieve email, the employees connect to an external mail server.

Creating an antivirus profile

Most antivirus settings are configured in an antivirus profile. Antivirus profiles are selected in firewall policies. This way, you can create multiple antivirus profiles, and tailor them to the traffic controlled by the security policy in which they are selected. In this example, you will create one antivirus profile.

To create an antivirus profile — web-based manager

- 1 Go to *UTM Profiles > AntiVirus > Profile*.
- 2 Select *Create New*.
- 3 In the *Name* field, enter `basic_antivirus`.
- 4 In the *Comments* field, enter `Antivirus protection for web and email traffic`.
- 5 Select the *Virus Scan* check boxes for the *HTTP*, *IMAP*, *POP3*, and *SMTP* traffic types.
- 6 Select *OK* to save the antivirus profile.

To create an antivirus profile — CLI

```
config antivirus profile
edit basic_antivirus
set comment "Antivirus protection for web and email traffic"
config http
set options scan
end
config imap
set options scan
end
```

```
config pop3
  set options scan
end
config smtp
  set options scan
end
end
```

Selecting the antivirus profile in a security policy

An antivirus profile directs the FortiGate unit to scan network traffic only when it is selected in a security policy. When an antivirus profile is selected in a security policy, its settings are applied to all the traffic the security policy handles.

To select the antivirus profile in a security policy — web-based manager

- 1 Go to *Policy > Policy > Policy*.
- 2 Select a policy.
- 3 Select the *Edit* icon.
- 4 Enable *UTM*.
- 5 Select `default` from the *Protocol Options* list.
UTM can not be enabled without selecting a protocol options profile. A default profile is provided.
- 6 Select the *Enable AntiVirus* option.
- 7 Select the `basic_antivirus` profile from the list.
- 8 Select *OK* to save the security policy.

To select the antivirus profile in a security policy — CLI

```
config firewall policy
  edit 1
    set utm-status enable
    set profile-protocol-options default
    set av-profile basic_antivirus
  end
```

HTTP, IMAP, POP3, and SMTP traffic handled by the security policy you modified will be scanned for viruses. A small office may have only one security policy configured. If you have multiple policies, consider enabling antivirus scanning for all of them.

Protecting your network against malicious email attachments

Grayware is commonly delivered by email or the web. The Example.com corporation has been the victim of multiple greyware infections in the past. Now that the company has a FortiGate unit protecting its network, you (Example.com's system administrator) can configure the unit to scan email and web traffic to filter out greyware attachments.

Enabling antivirus scanning in the antivirus profile

The primary means to avoid viruses is to configure the FortiGate unit to scan email and web traffic for virus signatures. You enable virus scanning in the antivirus profile and then select the antivirus profile in firewall policies that control email traffic.

To enable antivirus scanning in the antivirus profile

- 1 Go to *UTM Profiles > AntiVirus > Profile*.

- 2 Select *Create New* to add a new antivirus profile, or select the *Edit* icon of an existing antivirus profile.
- 3 Select the *Virus Scan* check box for *HTTP* to scan web traffic for viruses.
- 4 Select the *Virus Scan* check box for *IMAP*, *POP3*, and *SMTP* to scan all email protocols for viruses.
- 5 Select *OK* to save the antivirus profile.

Enabling grayware scanning

Grayware can also threaten Example.com's network. Viruses, email messages and the web are often the means by which grayware infections are delivered.

To enable grayware scanning

- 1 Go to *UTM Profiles > AntiVirus > Virus Database*.
- 2 Select *Enable Grayware Detection*.
- 3 Select *Apply*.

When *Enable Grayware Detection* is selected, virus scanning will also include grayware scanning. Any traffic scanned for viruses will also be scanned for grayware.

Selecting the antivirus profile in a security policy

An antivirus profile directs the FortiGate unit to scan network traffic only when it is selected in a security policy. When an antivirus profile is selected in a security policy, its settings are applied to all the traffic the security policy handles.

To select the antivirus profile in a security policy

- 1 Go to *Policy > Policy > Policy*.
- 2 Select the policy that controls the network traffic controlling email traffic.
- 3 Select the *Edit* icon.
- 4 Enable *UTM*.
- 5 Select the *Enable AntiVirus* option.
- 6 Select the antivirus profile from the list.
- 7 Select *OK* to save the security policy.

AntiVirus interface reference

The following explains the antivirus options that you can configure in the Antivirus menu. When configuring a profile, you can apply an antivirus profile to a firewall policy for HTTP, FTP, IMAP, POP3, SMTP, IM, and NNTP sessions. If your unit supports SSL content scanning and inspection you can also configure antivirus protection for HTTPS, IMAPS, POP3S, and SMTPS sessions.

This topic includes the following:

- [Profile](#)
- [Virus Database](#)

Profile

From the Profile submenu, you can configure antivirus profiles that are then applied to firewall policies. A profile is specific configuration information that defines how the traffic within a policy is examined and what action may be taken based on the examination.

You can create multiple antivirus profiles for different antivirus scanning requirements. For example, you create an antivirus profile that specifies only virus scanning for POP3 which you then apply to the out-going firewall policy. You can also choose specific protocols, such as POP3, that will be blocked and then archived by the unit. This option is available only in the CLI.

Within antivirus profiles, you can also choose specific protocols to be blocked and then archive them. This is available only in the CLI.

Antivirus profile configuration settings

The following are antivirus profile configuration settings in *UTM Profiles > Antivirus > Profile*.

Profile page Lists each individual antivirus profile that you created. On this page, you can edit, delete or create a new antivirus profile. You are redirected to this page when you select <i>View List</i> on the Edit Antivirus Profile page. Note: If you want to configure the profile to block and archive specific protocols, use the <code>options</code> value in the <code>config antivirus profile</code> command in the CLI.	
Create New	Creates a new antivirus profile. When you select <i>Create New</i> , you are automatically redirected to the New Antivirus Profile page.
Edit	Modifies settings within the antivirus profile. When you select <i>Edit</i> , you are automatically redirected to the Edit Antivirus Profile page.
Delete	Removes an antivirus profile from the list on the Profile page. To remove multiple antivirus profiles from within the list, on the Antivirus Profile page, in each of the rows of the profiles you want to remove, select the check box and then select <i>Delete</i> . To remove all antivirus profiles in the list, on the Antivirus Profile page, select the check box in the check box column, and then select <i>Delete</i> .
Name	The name of the antivirus profile.
Comments	A description for the antivirus profile.

Ref.	<p>Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a firewall policy; on the Profile page (<i>UTM Profiles > Antivirus > Profile</i>), 1 appears in <i>Ref.</i>.</p> <p>To view the location of the referenced object, select the number in <i>Ref.</i>, and the Object Usage window appears displaying the various locations of the referenced object.</p> <p>To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:</p> <ul style="list-style-type: none"> • View the list page for these objects – automatically redirects you to the list page where the object is referenced at. • Edit this object – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • View the details for this object – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy, and that firewall policy's settings appear within the table.
<p>New Antivirus Profile page</p> <p>Provides settings for configuring a new antivirus profile. This page also allows you to configure quarantine settings for including a virus sender to the Banned User List.</p> <p>This page appears when you select <i>Create New</i> on the Edit Antivirus Profile page. If you are on the Profile page, and you select <i>Create New</i>, you will be redirected to the <i>New Antivirus Profile</i> page.</p> <p>Note: Logging is enabled in the CLI.</p>	
Name	Enter a name for the profile. If you are editing an existing antivirus profile and want to change the name, enter a new name in this field. You must select <i>OK</i> to save these changes.
Comments	Enter a description for the profile; this is optional. If you are editing an existing antivirus profile and want to change the description, enter the changes in this field. You must select <i>OK</i> to save the changes.
Virus Scan and Removal	Select any of the following to have the unit scan for viruses when the available protocols are used for web (Internet activity, for example HTTP), email (for example, POP3 or POP3S), and transferring files (for example, FTP).
Quarantine	<p>Select to enable the quarantine of detected viruses.</p> <p>Quarantined information is available in <i>Log&Report > Log & Archive Access</i>.</p>

Virus Database

The unit contains multiple antivirus databases for you to choose from, so that you can get the maximum protection that you need for your network environment. The Virus Database, located in *UTM Profiles > Antivirus > Virus Database*, is used to detect viruses in network traffic. The databases are available on the Virus Database page:

- Regular Virus Database
- Extended Virus Database
- Extreme Virus Database
- Flow-based Virus Database

On the Virus Database page, you can also enable grayware detection. This grayware detection includes adware, dial, downloader, hacker tool, keylogger, RAT, and spyware.

The extended database provides “in the wild” viruses as well as a large collection of zoo viruses that have not yet been seen in current virus studies. An enhanced security environment is best suited for this type of database. The flow-based database provides “in the wild” viruses as well as some commonly seen viruses on the network. Flow-based virus scanning is an alternative to the file-based virus scanning, providing better performance but lower coverage rates than the file-based virus scan.

The extreme antivirus database allows scanning for both “in the wild” and “zoo” viruses that are no longer seen in recent studies as well as all available signatures that are currently supported. The extreme database provides flexibility, providing the maximum protection without sacrificing performance and is suited to an enhanced security environment. The extreme antivirus database is available only on models that have AMC-enabled platforms and large capacity hard drives.

The flow-based antivirus database helps to detect malware using IPS. This database includes “in the wild” viruses along with some commonly seen viruses on the network. The flow-based antivirus database provides an alternative to the file-based virus scan while also providing better performance.

The FortiGuard virus definitions are updated when the unit receives a new version of FortiGuard antivirus definitions from the FDN.



The FDN updates only the virus database selected in UTM Profiles > AntiVirus > Virus Database. If you’ve configured the use of other databases in antivirus profiles that are selected in security policies, those will also be updated by the FDN. To save bandwidth, antivirus databases that are in use are not updated.

The [FortiGuard Center Virus Encyclopedia](#) contains detailed descriptions of the viruses, worms, trojans, and other threats that can be detected and removed by your unit using the information in the FortiGuard virus definitions.

The FortiGuard AV definitions are updated automatically from the FortiGuard Distribution Network (FDN). Automatic antivirus definition updates are configured from the FDN by going to *System > Maintenance > FortiGuard*. You can also update the antivirus definitions manually from the system dashboard by going to *System > Dashboard > Status*.



If virtual domains are enabled, you must configure antivirus settings in antivirus profiles separately for each virtual domain. Grayware settings can only be enabled or disabled when running FortiOS 4.0 MR2 or higher on the unit.



Email filter

This section describes how to configure FortiGate email filtering for IMAP, POP3, and SMTP email. Email filtering includes both spam filtering and filtering for any words or files you want to disallow in email messages. If your FortiGate unit supports SSL content scanning and inspection, you can also configure spam filtering for IMAPS, POP3S, and SMTPS email traffic.

The following topics are included in this section:

- [Email filter concepts](#)
- [Enable email filter](#)
- [Configure email traffic types to inspect](#)
- [Configure the spam action](#)
- [Configure the tag location](#)
- [Configure the tag format](#)
- [Configure FortiGuard email filters](#)
- [Configure local email filters](#)
- [Email filter examples](#)

Email filter concepts

You can configure the FortiGate unit to manage unsolicited commercial email by detecting and identifying spam messages from known or suspected spam servers.

The FortiGuard Antispam Service uses both a sender IP reputation database and a spam signature database, along with sophisticated spam filtering tools, to detect and block a wide range of spam messages. Using FortiGuard Antispam email filter profile settings, you can enable IP address checking, URL checking, email checksum checking, and spam submission. Updates to the IP reputation and spam signature databases are provided continuously via the global FortiGuard Distribution Network.

From the [FortiGuard Antispam Service](#) page in the FortiGuard Center, you can find out whether an IP address is blacklisted in the FortiGuard antispam IP reputation database, or whether a URL or email address is in the signature database.

Email filter techniques

The FortiGate unit has a number of techniques available to help detect spam. Some use the FortiGuard Antispam Service and require a subscription. The remainder use your DNS servers or use lists that you must maintain.

FortiGuard IP address check

The FortiGate unit queries the FortiGuard Antispam Service to determine if the IP address of the client delivering the email is blacklisted. A match will cause the FortiGate unit to treat delivered messages as spam.

The default setting of the `smtp-spamhdrip` CLI command is `disable`. If enabled, the FortiGate unit will check all the IP addresses in the header of SMTP email against the FortiGuard Antispam Service. For more information, see the [FortiGate CLI Reference](#).

FortiGuard URL check

The FortiGate unit queries the FortiGuard Antispam service to determine if any URL in the message body is associated with spam. If any URL is blacklisted, the FortiGate unit determines that the email message is spam.

Detect phishing URLs in email

The FortiGate unit sends the URL links in email messages to FortiGuard to determine if the links are associated with a known phishing site. If such a link is detected, the link is removed from the message. The URL remains, but it is no longer a selectable hyperlink.

FortiGuard email checksum check

The FortiGate unit sends a hash of an email to the FortiGuard Antispam server, which compares the hash to hashes of known spam messages stored in the FortiGuard Antispam database. If the hash results match, the email is flagged as spam.

FortiGuard spam submission

Spam submission is a way you can inform the FortiGuard AntiSpam service of non-spam messages incorrectly marked as spam. When you enable this setting, the FortiGate unit adds a link to the end of every message marked as spam. You then select this link to inform the FortiGuard AntiSpam service when a message is incorrectly marked.

IP address black/white list check

The FortiGate unit compares the IP address of the client delivering the email to the addresses in the IP address black/white list specified in the email filter profile. If a match is found, the FortiGate unit will take the action configured for the matching black/white list entry against all delivered email.

The default setting of the `smtp-spamhdrip` CLI command is `disable`. If enabled, the FortiGate unit will check all the IP addresses in the header of SMTP email against the specified IP address black/white list. For more information, see the [FortiGate CLI Reference](#).

HELO DNS lookup

The FortiGate unit takes the domain name specified by the client in the HELO greeting sent when starting the SMTP session and does a DNS lookup to determine if the domain exists. If the lookup fails, the FortiGate unit determines that any messages delivered during the SMTP session are spam.

Email address black/white list check

The FortiGate unit compares the sender email address, as shown in the message envelope MAIL FROM, to the addresses in the email address black/white list specified in the email filter profile. If a match is found, the FortiGate unit will take the action configured for the matching black/white list entry.

Return email DNS check

The FortiGate unit performs a DNS lookup on the reply-to domain to see if there is an A or MX record. If no such record exists, the message is treated as spam.

Banned word check

The FortiGate unit blocks email messages based on matching the content of the message with the words or patterns in the selected spam filter banned word list.

Order of spam filtering

The FortiGate unit checks for spam using various filtering techniques. The order in which the FortiGate unit uses these filters depends on the mail protocol used.

Filters requiring a query to a server and a reply (FortiGuard Antispam Service and DNSBL/ORDBL) are run simultaneously. To avoid delays, queries are sent while other filters are running. The first reply to trigger a spam action takes effect as soon as the reply is received.

Each spam filter passes the email to the next if no matches or problems are found. If the action in the filter is *Mark as Spam*, the FortiGate unit tags the email as spam according to the settings in the email filter profile.

For SMTP and SMTPS, if the action is discard, the email message is discarded or dropped.

If the action in the filter is *Mark as Clear*, the email is exempt from any remaining filters. If the action in the filter is *Mark as Reject*, the email session is dropped. Rejected SMTP or SMTPS email messages are substituted with a configurable replacement message.

Order of SMTP and SMTPS spam filtering

The FortiGate unit scans SMTP and SMTPS email for spam in the order given below. SMTPS spam filtering is available on FortiGate units that support SSL content scanning and inspection.

- 1 IP address black/white list (BWL) check on last hop IP
- 2 DNSBL & ORDBL check on last hop IP, FortiGuard Antispam IP check on last hop IP, HELO DNS lookup
- 3 MIME headers check, E-mail address BWL check
- 4 Banned word check on email subject
- 5 IP address BWL check (for IPs extracted from "Received" headers)
- 6 Banned word check on email body
- 7 Return email DNS check, FortiGuard Antispam email checksum check, FortiGuard Antispam URL check, DNSBL & ORDBL check on public IP extracted from header.

Order of IMAP, POP3, IMAPS and POP3S spam filtering

The FortiGate unit scans IMAP, POP3, IMAPS and POP3S email for spam in the order given below. IMAPS and POP3S spam filtering is available on FortiGate units that support SSL content scanning and inspection.

- 1 MIME headers check, E-mail address BWL check
- 2 Banned word check on email subject
- 3 IP BWL check
- 4 Banned word check on email body
- 5 Return email DNS check, FortiGuard Antispam email checksum check, FortiGuard Antispam URL check, DNSBL & ORDBL check.

Enable email filter

Unlike antivirus protection, no single control enables all email filtering. Your FortiGate unit uses many techniques to detect spam; some may not be appropriate for every situation. For this reason, when you enable email filtering, you must then choose when techniques are applied to email traffic.

To enable email traffic inspection

- 1 Go to *UTM Profiles > Email Filter > Profile*.
- 2 The default email filter profile is presented. To edit another profile, select it from the drop down in the *Edit Email Filter Profile* title bar.
- 3 Select *Enable Spam Detection and Filtering*.
- 4 Select *Apply*.

Once you allow the FortiGate unit to examine one or more types of email traffic, you can enable any of the individual email filtering techniques.

Configure email traffic types to inspect

The FortiGate unit can examine IMAP, POP3, and SMTP email traffic. If your FortiGate unit supports content inspection, it can also examine IMAPS, POP3S, and SMTPS traffic. You can select which types of email traffic are examined by each email filter profile.

To select the email traffic types to inspect

- 1 Go to *UTM Profiles > Email Filter > Profile*.
- 2 The default email filter profile is presented. To edit another profile, select it from the drop down in the *Edit Email Filter Profile* title bar.
- 3 If *Enable Spam Detection and Filtering* is enabled, the row immediately below shows a check box for each traffic type. Select the traffic types you want the FortiGate unit to examine when using this email filter profile.
- 4 Select *Apply*.

The traffic types you enable will be examined according to the settings in the email filter profile.

Configure the spam action

When spam is detected, the FortiGate unit will deal with it according to the *Spam Action* setting in the email filter profile. Note that POP3S, IMAPS and SMTPS spam filtering is available only on FortiGate units that support SSL content scanning and inspection. POP3, IMAP, POP3S and IMAPS mail can only be tagged. SMTP and SMTPS mail can be set to *Discard* or *Tagged*:

- **Discard:** When the spam action is set to *Discard*, messages detected as spam are deleted. No notification is sent to the sender or recipient.
- **Tagged:** When the spam action is set to *Tagged*, messages detected as spam are labelled and delivered normally. The text used for the label is set in the *Tag Format* field and the label is placed in the subject or the message header, as set with the *Tag Location* option.

To configure the spam action

- 1 Go to *UTM Profiles > Email Filter > Profile*.
- 2 The default email filter profile is presented. To edit another profile, select it from the drop down in the *Edit Email Filter Profile* title bar.
- 3 The *Spam Action* row has a drop-down selection under the SMTP and SMTPS traffic type. Select *Discard* or *Tagged*.

No selection is available for POP3, IMAP, POP3S or IMAPS traffic. *Tagged* is the only applicable action for those traffic types.

By default, the tag location for any traffic set to *Tagged* is *Subject* and the tag format is *Spam*. If you want to change these settings, continue with [“Configure the tag location” on page 53](#) and [“Configure the tag format” on page 53](#).

- 4 Select *Apply*.

Select the edited email filter profile in a security policy, and the traffic controlled by the security policy will be scanned according to the settings you configured. You may select the email filter profile in more than one security policy if required.

Configure the tag location

When the spam action is set to *Tagged*, the *Tag Location* setting determines where the tag is applied in the message.

To configure the tag location

- 1 Go to *UTM Profiles > Email Filter > Profile*.
- 2 The default email filter profile is presented. To edit another profile, select it from the drop down in the *Edit Email Filter Profile* title bar.
- 3 The *Tag Location* row has two options for each traffic type. Note that if the spam action for SMTP traffic is set to discard, the tag location will not be available. Select the tag location:
 - *Subject*: The FortiGate unit inserts the tag at the beginning of the message subject. For example, if the message subject is “Buy stuff!” and the tag is “[spam]”, the new message subject is “[spam] Buy stuff!” if the message is detected as spam.
 - *MIME*: The FortiGate unit inserts the tag into the message header. With most mail readers and web-based mail services, the tag will not be visible. Despite this, you can still set up a rule based on the presence or absence of the tag.
- 4 Select *Apply*.

Configure the tag format

When the spam action is set to *Tagged*, the *Tag Format* setting determines what text is used as the tag applied to the message.

To configure the tag format

- 1 Go to *UTM Profiles > Email Filter > Profile*.
- 2 The default email filter profile is presented. To edit another profile, select it from the drop down in the *Edit Email Filter Profile* title bar.

- 3 The *Tag Format* row has a field for each traffic type. Note that if the spam action for SMTP traffic is set to discard, the tag format will not be available. Enter the text the FortiGate unit will use as the tag for each traffic type.
- 4 Select *Apply*.

Configure FortiGuard email filters

FortiGuard email filtering techniques use FortiGuard services to detect the presence of spam among your email. A FortiGuard subscription is required to use the FortiGuard email filters.

Enabling FortiGuard IP address checking

When you enable FortiGuard IP address checking, your FortiGate unit will submit the IP address of the client to the FortiGuard service for checking. If the IP address exists in the FortiGuard IP address black list, your FortiGate unit will treat the message as spam.

To enable FortiGuard IP address checking

- 1 Go to *UTM Profiles > Email Filter > Profile*.
- 2 The default email filter profile is presented. To edit another profile, select it from the drop down in the *Edit Email Filter Profile* title bar.
- 3 Under the heading *FortiGuard Spam Filtering*, select *IP Address Check*.
- 4 Select *Apply*.

Select the edited email filter profile in a security policy, and the traffic controlled by the security policy will be scanned according to the settings you configured. You may select the email filter profile in more than one security policy if required.

Enabling FortiGuard URL checking

When you enable FortiGuard IP address checking, your FortiGate unit will submit all URLs appearing in the email message body to the FortiGuard service for checking. If a URL exists in the FortiGuard URL black list, your FortiGate unit will treat the message as spam.

To enable FortiGuard URL checking

- 1 Go to *UTM Profiles > Email Filter > Profile*.
- 2 The default email filter profile is presented. To edit another profile, select it from the drop down in the *Edit Email Filter Profile* title bar.
- 3 Under the heading *FortiGuard Spam Filtering*, select *URL Check*.
- 4 Select *Apply*.

Select the edited email filter profile in a security policy, and the traffic controlled by the security policy will be scanned according to the settings you configured. You may select the email filter profile in more than one security policy if required.

Enabling FortiGuard phishing URL detection

When you enable FortiGuard phishing URL detection, your FortiGate unit will submit all URL hyperlinks appearing in the email message body to the FortiGuard service for checking. If a URL exists in the FortiGuard URL phishing list, your FortiGate unit will remove the hyperlink from the message. The URL will remain in place, but it will no longer be a selectable hyperlink.

To enable FortiGuard phishing URL detection

- 1 Go to *UTM Profiles > Email Filter > Profile*.
- 2 The default email filter profile is presented. To edit another profile, select it from the drop down in the *Edit Email Filter Profile* title bar.
- 3 Under the heading *FortiGuard Spam Filtering*, select *Detect Phishing URLs in Email*.
- 4 Select *Apply*.

Select the edited email filter profile in a security policy, and the traffic controlled by the security policy will be scanned according to the settings you configured. You may select the email filter profile in more than one security policy if required.

Enabling FortiGuard email checksum checking

When you enable FortiGuard email checksum checking, your FortiGate unit will submit a checksum of each email message to the FortiGuard service for checking. If a checksum exists in the FortiGuard checksum black list, your FortiGate unit will treat the message as spam.

To enable FortiGuard checksum checking

- 1 Go to *UTM Profiles > Email Filter > Profile*.
- 2 The default email filter profile is presented. To edit another profile, select it from the drop down in the *Edit Email Filter Profile* title bar.
- 3 Under the heading *FortiGuard Email Filtering*, select *E-mail Checksum Check*.
- 4 Select *Apply*.

Select the edited email filter profile in a security policy, and the traffic controlled by the security policy will be scanned according to the settings you configured. You may select the email filter profile in more than one security policy if required.

Enabling FortiGuard spam submission

When you enable FortiGuard email checksum checking, your FortiGate unit will append a link to the end of every message detected as spam. This link allows email users to “correct” the FortiGuard service by informing it that the message is not spam.



Carefully consider the use of the *Spam submission* option on email leaving your network. Users not familiar with the feature may click the link on spam messages because they are curious. This will reduce the accuracy of the feature.

To enable FortiGuard Spam submission

- 1 Go to *UTM Profiles > Email Filter > Profile*.
- 2 The default email filter profile is presented. To edit another profile, select it from the drop down in the *Edit Email Filter Profile* title bar.
- 3 Under the heading *FortiGuard Email Filtering*, select *Spam Submission*.
- 4 Select *Apply*.

Select the edited email filter profile in a security policy, and the traffic controlled by the security policy will be scanned according to the settings you configured. You may select the email filter profile in more than one security policy if required.

Configure local email filters

Local email filtering techniques use your own resources, whether DNS checks or IP address and email address lists that you maintain.

Enabling IP address black/white list checking

When you enable IP address black/white list checking, your FortiGate unit will compare the client IP address with the IP address black/white list specified in the email filter profile. If the client IP address exists, the FortiGate unit acts according to the action configured for the IP address in the list: allow the message, reject it, or mark it as spam.

The next two topics describe adding and configuring the IP address black/white list that you will need before you can enable the checking. If you already have this list, go to [“Enabling the IP address black/white list checking” on page 57](#).

Creating an IP address black/white list

Before you can enable IP address black/white list spam filtering in the email filter profile, you must create an IP address black/white list.

To create an IP address black/white list

- 1 Go to *UTM Profiles > Email Filter > IP Address*.
- 2 Select *Create New*.
- 3 Enter a name for the IP address list.
- 4 Optionally, enter a description or comments about the list.
- 5 Select *OK* to save the IP address black/white list.

When a new IP address black/white list is created, it is empty. To perform any actions, you must add IP addresses to the list.

Adding addresses to an IP address black/white list

Each IP address black/white list contains a number of IP addresses, each having a specified action. When the FortiGate unit accepts mail from a client with an IP address on the IP address black/white list specified in the active email filter profile, it performs the action specified for the address.

To add an address to an IP address black/white list

- 1 Go to *UTM Profiles > Email Filter > IP Address*.
- 2 Select the list to which you want to add an address and choose *Edit*.
- 3 Select *Create New*.
- 4 Enter the address or netmask in the IP/netmask field.

- 5 Select the action:
 - *Mark as Clear*: Messages from clients with matching IP addresses will be allowed, bypassing further email filtering.
 - *Mark as Reject*: Messages from clients with matching IP addresses will be rejected. The FortiGate unit will return a reject message to the client. *Mark as Reject* only applies to mail delivered by SMTP. If an IP address black/white list is used with POP3 or IMAP mail, addresses configured with the *Mark as Reject* action will be marked as spam.
 - *Mark as Spam*: Messages from clients with matching IP addresses will be treated as spam, subject to the action configured in the applicable email filter profile. For more information, see [“Configure the spam action” on page 52](#).
- 6 By default, the address is enabled and the FortiGate unit will perform the action if the address is detected. To disable checking for the address, clear the *Enable* check box.
- 7 Select OK.

Enabling the IP address black/white list checking

Once you have created a black/white list and added the IP addresses, you can enable IP address the checking.

To enable IP address black/white list checking

- 1 Go to *UTM Profiles > Email Filter > Profile*.
- 2 The default email filter profile is presented. To edit another profile, select it from the drop down in the *Edit Email Filter Profile* title bar.
- 3 Under the heading *Local Spam Filtering*, select *IP Address BWL Check*.
- 4 Select the IP address black/white list to use from the drop-down list.
- 5 Select *Apply*.

Select the edited email filter profile in a security policy, and the traffic controlled by the security policy will be scanned according to the settings you configured. You may select the email filter profile in more than one security policy if required.

Enabling HELO DNS lookup

Whenever a client opens an SMTP session with a server, the client sends a HELO command with the client domain name. When you enable HELO DNS lookup, your FortiGate unit will take the domain the client submits as part of the HELO greeting and send it to the configured DNS. If the domain does not exist, your FortiGate unit will treat all messages the client delivers as spam.

The HELO DNS lookup is available only for SMTP traffic.

To enable HELO DNS lookup

- 1 Go to *UTM Profiles > Email Filter > Profile*.
- 2 The default email filter profile is presented. To edit another profile, select it from the drop down in the *Edit Email Filter Profile* title bar.
- 3 Under the heading *Local Spam Filtering*, select *HELO DNS Lookup*.
- 4 Select *Apply*.

Select the edited email filter profile in a security policy, and the traffic controlled by the security policy will be scanned according to the settings you configured. You may select the email filter profile in more than one security policy if required.

Enabling email address black/white list checking

When you enable email address black/white list checking, your FortiGate unit will compare the sender email address with the email address black/white list specified in the email filter profile. If the sender email address exists, the FortiGate unit acts according to the action configured for the email address in the list: allow the message or mark it as spam.

The next two topics describe adding and configuring the email address black/white list that you will need before you can enable the checking. If you already have this list, go to [“Enabling email address black/white list checking” on page 59](#).

Creating an email address black/white list

Before you can enable email address black/white list spam filtering in the email filter profile, you must create an email address black/white list.

To create an email address black/white list

- 1 Go to *UTM Profiles > Email Filter > E-mail Address*.
- 2 Select *Create New*.
- 3 Enter a name for the email address list.
- 4 Optionally, enter a description or comments about the list.
- 5 Select *OK* to save the email address black/white list.

When a new IP address back/white list is created, it is empty. To perform any actions, you must add email addresses to the list.

Adding addresses to an email address black/white list

Each email address black/white list may contain a number of email addresses, each having a specified action. When the FortiGate unit accepts an email message from a client with a reply-to address that appears in the email address black/white list specified in the active email filter profile, it performs the action specified for the email message.

To add an address to an email address black/white list

- 1 Go to *UTM Profiles > Email Filter > E-mail Address*.
- 2 Select the *Edit* icon of the list to which you want to add an address.
- 3 Select *Create New*.
- 4 Enter the email address in the *Email Address* field.
- 5 If you need to enter a pattern in the *Email Address* field, select whether to use wildcards or regular expressions to specify the pattern.

Wildcard uses an asterisk (“*”) to match any number of any character. For example, *@example.com will match all addresses ending in @example.com.

Regular expressions use Perl regular expression syntax. See <http://perldoc.perl.org/perlretut.html> for detailed information about using Perl regular expressions.

- 6 Select the action:
 - *Mark as Spam*: Messages with matching reply-to email addresses will be treated as spam, subject to the action configured in the applicable email filter profile. For more information, see [“Configure the spam action” on page 52](#).
 - *Mark as Clear*: Messages with matching reply-to addresses will be allowed, bypassing further email filtering.

- 7 By default, the address is enabled and the FortiGate unit will perform the action if the address is detected. To disable checking for the address, clear the *Enable* check box.
- 8 Select *OK* to save the address.

Enabling email address black/white list checking

Once you have created a black/white list and added the email addresses, you can enable the checking.

To enable email address black/white list checking

- 1 Go to *UTM Profiles > Email Filter > Profile*.
- 2 The default email filter profile is presented. To edit another profile, select it from the drop down in the *Edit Email Filter Profile* title bar.
- 3 Under the heading *Local Spam Filtering*, select *E-mail Address BWL Check*.
- 4 Select the email address black/white list to use from the drop-down list.
- 5 Select *Apply*.

Select the edited email filter profile in a security policy, and the traffic controlled by the security policy will be scanned according to the settings you configured. You may select the email filter profile in more than one security policy if required.

Enabling return email DNS checking

When you enable return email DNS checking, your FortiGate unit will take the domain in the reply-to email address and send it to the configured DNS. If the domain does not exist, your FortiGate unit will treat the message as spam.

To enable return email DNS check

- 1 Go to *UTM Profiles > Email Filter > Profile*.
- 2 The default email filter profile is presented. To edit another profile, select it from the drop down in the *Edit Email Filter Profile* title bar.
- 3 Under the heading *Local Spam Filtering*, select *Return E-mail DNS Check*.
- 4 Select *Apply*.

Select the edited email filter profile in a security policy, and the traffic controlled by the security policy will be scanned according to the settings you configured. You may select the email filter profile in more than one security policy if required.

Enabling banned word checking

When you enable banned word checking, your FortiGate unit will examine the email message for words appearing in the banned word list specified in the email filter profile. If the total score of the banned word discovered in the email message exceeds the threshold value set in the email filter profile, your FortiGate unit will treat the message as spam.

When determining the banned word score total for an email message, each banned word score is added once no matter how many times the word appears in the message.

The next two topics describe adding and configuring the banned word list that you will need before you can enable the checking. If you already have this list, go to [“Enabling banned word checking” on page 62](#).

How content is evaluated

Every time the banned word filter detects a pattern in an email message, it adds the pattern score to the sum of scores for the message. You set this score when you create a new pattern to block content. The score can be any number from zero to 99999. Higher scores indicate more offensive content. When the total score equals or exceeds the threshold, the email message is considered as spam and treated according to the spam action configured in the email filter profile. The score for each pattern is counted only once, even if that pattern appears many times in the email message. The default score for banned word patterns is 10 and the default threshold is 10. This means that by default, an email message is blocked by a single match.

A pattern can be part of a word, a whole word, or a phrase. Multiple words entered as a pattern are treated as a phrase. The phrase must appear as entered to match. You can also use wildcards or regular expressions to have a pattern match multiple words or phrases.

For example, the FortiGate unit scans an email message that contains only this sentence: "The score for each word or phrase is counted only once, even if that word or phrase appears many times in the email message."

Banned word pattern	Pattern type	Assigned score	Score added to the sum for the entire page	Comment
word	Wildcard	20	20	The pattern appears twice but multiple occurrences are only counted once.
word phrase	Wildcard	20	0	Although each word in the phrase appears in the message, the words do not appear together as they do in the pattern. There are no matches.
word*phrase	Wildcard	20	20	The wildcard represents any number of any character. A match occurs as long as "word" appears before "phrase" regardless of what is in between them.
mail*age	Wildcard	20	20	Since the wildcard character can represent any characters, this pattern is a match because "email message" appears in the message.

In this example, the message is treated as spam if the banned word threshold is set to 60 or less.

Creating a banned word list

Before you can enable IP address black/white list spam filtering in the email filter profile, you must create an IP address black/white list.

To create an IP address black/white list

- 1 Go to *UTM Profiles > Email Filter > Banned Word*.
- 2 Select *Create New*.
- 3 Enter a name for the banned word list.
- 4 Optionally, enter a description or comments about the list.
- 5 Select *OK* to save the banned word list.

When a new banned word list is created, it is empty. To perform any actions, you must add words to the list.

Adding words to a banned word list

Each banned word list contains a number of words, each having a score, and specifying whether the email FortiGate unit will search for the word in the message subject, message body, or both.

When the FortiGate unit accepts an email message containing one or more words in the banned word list specified in the active email filter profile, it totals the scores of the banned words in the email message. If the total is higher than the threshold set in the email filter profile, the email message will be detected as spam. If the total score is lower than the threshold, the message will be allowed to pass as normal.

The score of a banned word present in the message will be counted toward the score total only once, regardless of how many times the word appears in the message.

To add words to a banned word list

- 1 Go to *UTM Profiles > Email Filter > Banned Word*.
- 2 Select the list to which you want to add a word.
- 3 Select *Edit*.
- 4 Select *Create New*.
- 5 Enter the word or the pattern in the *Pattern* field.
- 6 In the *Pattern Type* field, select whether you use wildcards or regular expressions.
Wildcard uses an asterisk (“*”) to match any number of any character. For example, *re** will match all words starting with “re”.
Regular expression uses Perl regular expression syntax. See <http://perldoc.perl.org/perlretut.html> for detailed information about using Perl regular expressions.
- 7 In the *Language* field, select the language.
- 8 Select where the FortiGate unit will check for the banned word. The options are *Body*, *Subject*, or *All*, which combines the other two options.
- 9 Enter a score. If the word appears in the message as determined by the *Where* setting, the score is added to the scores of all the other banned words appearing in the email message. If the score total is higher than the threshold set in the email filter profile, the email message will be detected as spam. If the total score is lower than the threshold, the message will be allowed to pass as normal.

10 By default, the banned word is enabled and will appear in the list. To disable checking for the banned word, clear the *Enable* check box.

11 Select *OK* to save the banned word.

Enabling banned word checking

Once you have created a black/white list and added the email addresses, you can enable the checking.

To enable banned word checking

- 1** Go to *UTM Profiles > Email Filter > Profile*.
- 2** The default email filter profile is presented. To edit another profile, select it from the drop down in the *Edit Email Filter Profile* title bar.
- 3** Under the heading *Local Spam Filtering*, select *Banned Word Check*.
- 4** Select the banned word list to use from the drop-down list.
- 5** Enter a threshold value. If the total score of the banned words appearing in the message exceeds this threshold, the FortiGate unit treats the message as spam.
- 6** Select *Apply*.

Select the edited email filter profile in a security policy, and the traffic controlled by the security policy will be scanned according to the settings you configured. You may select the email filter profile in more than one security policy if required.

Email filter examples

Configuring simple antispam protection

Small offices, whether they are small companies, home offices, or satellite offices, often have very simple needs. This example details how to enable antispam protection on a FortiGate unit located in a satellite office.

Creating an email filter profile

Most email filter settings are configured in an email filter profile. Email filter profiles are selected in firewall policies. This way, you can create multiple email filter profiles, and tailor them to the traffic controlled by the security policy in which they are selected. In this example, you will create one email filter profile.

To create an email filter profile — web-based manager

- 1** Go to *UTM Profiles > Email Filter > Profile*.
- 2** Select the *Create New* icon in the Edit Email Filter Profile window title.
- 3** In the *Name* field, enter `basic_emailfilter`.
- 4** Select *Enable Spam Detection and Filtering*.
- 5** Ensure that *IMAP*, *POP3*, and *SMTP* are selected in the header row.
These header row selections enable or disable examination of each email traffic type. When disabled, the email traffic of that type is ignored by the FortiGate unit and no email filtering options are available.
- 6** Under *FortiGuard Spam Filtering*, enable *IP Address Check*.
- 7** Under *FortiGuard Spam Filtering*, enable *URL Check*.
- 8** Under *FortiGuard Spam Filtering*, enable *E-mail Checksum Check*.

- 9 Select *OK* to save the email filter profile.

To create an email filter profile — CLI

```
config spamfilter profile
edit basic_emailfilter
set options spamfsip spamfsurl spamfschksum
end
```

Selecting the email filter profile in a security policy

An email filter profile directs the FortiGate unit to scan network traffic only when it is selected in a security policy. When an email filter profile is selected in a security policy, its settings are applied to all the traffic the security policy handles.

To select the email filter profile in a security policy — web-based manager

- 1 Go to *Policy > Policy > Policy*.
- 2 Select a policy.
- 3 Select the *Edit* icon.
- 4 Enable *UTM*.
- 5 Select the *Enable Email Filter* option.
- 6 Select the `basic_emailfilter` profile from the list.
- 7 Select *OK* to save the security policy.

To select the email filter profile in a security policy — CLI

```
config firewall policy
edit 1
set utm-status enable
set profile-protocol-options default
set spamfilter-profile basic_emailfilter
end
```

IMAP, POP3, and SMTP email traffic handled by the security policy you modified will be scanned for spam. Spam messages have the text “Spam” added to their subject lines. A small office may have only one security policy configured. If you have multiple policies, consider enabling spam scanning for all of them.

Blocking email from a user

Employees of the Example.com corporation have been receiving unwanted email messages from a former client at a company called example.net. All ties between the company and the client have been severed, but the messages continue. The FortiGate unit can be configured to prevent these messages from being delivered.

To create the email address list

- 1 Go to *UTM Profiles > Email Filter > E-mail Address*.
- 2 Select *Create New*.
- 3 Enter a name for the new email address list.
- 4 Optionally, enter a descriptive comment for the email address list.
- 5 Select *OK* to create the list.
- 6 Select *Create New* to add a new entry to the email address list.
- 7 Enter `*@example.net` in the *E-mail Address* field.

- 8 Leave *Pattern Type* set to the default, *Wildcard*.
- 9 Leave *Action* as *Mark as Spam* to have the FortiGate unit mark all messages from example.net as spam.

Now that the email address list is created, you must enable the email filter in the email filter profile.

To enable Email Filter

- 1 Go to *UTM Profiles > Email Filter > Profile*.
- 2 Select the email filter profile that is used by the firewall policies handling email traffic from the email filter profile drop down list.
- 3 In the row *Tag Location*, select *Subject* for all three mail protocols.
- 4 In the row *Tag Format*, enter *SPAM:* in all three fields.
- 5 Select *Enable Spam Detection and Filtering*.
- 6 Ensure that the check boxes labeled *IMAP*, *POP3*, and *SMTP* in the header row are selected.
- 7 Under *Local Spam Filtering*, enable *E-mail Address BWL Check* and select the email address list you created in the previous procedure from the drop down list.
- 8 Select *OK*.

When this email filter profile is selected in a security policy, the FortiGate unit will add "SPAM:" to the subject of any email message from an address ending with @example.net for all email traffic handled by the security policy. Recipients can ignore the message or they can configure their email clients to automatically delete messages with "SPAM:" in the subject.

Email Filter interface reference

Reports page	
Provides settings for configuring a report that you generated. The information for these reports are taken from a web filter profile. You must first configure a web filter profile before you can generate a report.	
Web Filter Profile	Select the web filter profile that you want to see a report based on.
Clear report data	Removes all data within the report that you are currently viewing.
Report Type	Select the time period for the report. Choose from <i>Hour</i> , <i>Day</i> , or <i>All</i> .
Report Range	Select the time range (format is in the 24 hour clock) or day range (from six days ago to today) for the report. For example, for an "hour" report type with a range of 13 to 16, the result is a category block report for 1 pm and 4 pm today. For a "day" report type with a range of 0 to 3, the result is a category block report for three days ago from today.
Get Report	Select to generate a report.
The generated report includes the following columns that appear below the pie chart on the Reports page:	
Category	The category for which the statistic was generated.

Allowed	The number of allowed web addresses accessed in the selected time frame.
Blocked	The number of blocked web addresses accessed in the selected time frame.
Logged	The logged web filter information.
Overridden	The blocked instances where an override was allowed.

If your unit supports SSL content scanning and inspection you can also configure email filtering for IMAPS, POP3S, and SMTPS email traffic.

You can configure the unit to manage unsolicited commercial email by identifying spam messages from known or suspected spam servers.

The [FortiGuard Antispam Service](#) uses both a sender IP reputation database and a spam signature database, along with sophisticated spam filtering tools, to detect and block a wide range of spam messages. Using FortiGuard Email filtering profile settings you can enable IP address checking, URL checking, E-mail checksum checking, and Spam submission. Updates to the IP reputation and spam signature databases are provided continuously from the global FortiGuard distribution network.

From the [FortiGuard Antispam Service](#) page in the FortiGuard center you can use IP and signature lookup to check whether an IP address is blacklisted in the FortiGuard antispam IP reputation database, or whether a URL or email address is in the signature database.

This topic contains the following:

- [Order of email filteringProfile](#)
- [Banned Word](#)
- [IP Address](#)
- [Email Filter interface reference](#)

Order of email filtering

Email filtering uses various filtering techniques. The order the unit uses these filters depends on the mail protocol that is used.

Filters requiring a query to a server and a reply (FortiGuard Antispam Service and DNSBL/ORDBL) are run simultaneously. To avoid delays, queries are sent while other filters are running. The first reply to trigger a spam action takes effect as soon as the reply is received.

Each filter passes the email to the next if no matches or problems are found. If the action in the filter is Mark as Spam, the Fortinet unit tags as spam the email according to the settings in the email filter profile.

For SMTP and SMTPS if the action is discard the email message is discarded or dropped.

If the action in the filter is *Mark as Clear*, the email is exempt from any remaining filters. If the action in the filter is *Mark as Reject*, the email session is dropped. Rejected SMTP or SMTPS email messages are substituted with a configurable replacement message.

Order of SMTP and SMTPS email filtering

SMTPS email filtering is available on units that support SSL content scanning and inspection.

- 1 IP address BWL check on last hop IP.

- 2 DNSBL & ORDBL check on last hop IP, FortiGuard Email Filtering IP address check on last hop IP, HELO DNS lookup.
- 3 MIME headers check, E-mail address BWL check.
- 4 Banned word check on email subject.
- 5 IP address BWL check (for IPs extracted from “Received” headers).
- 6 Banned word check on email body.
- 7 Return email DNS check, FortiGuard Antispam email checksum check, FortiGuard Email Filtering URL check, DNSBL & ORDBL check on public IP extracted from header.

Order of IMAP, POP3, IMAPS and POP3S email filtering

IMAPS and POP3S email filtering is available on units the support SSL content scanning and inspection.

- 1 MIME headers check, Email address BWL check.
- 2 Banned word check on email subject.
- 3 IP BWL check.
- 4 Banned word check on email body.
- 5 Return email DNS check, FortiGuard Email Filtering email checksum check, FortiGuard Email Filtering URL check, DNSBL & ORDBL check.

Profile

The Profile menu allows you to configure email filter profiles for applying to firewall policies. A profile is specific information that defines how the traffic within a policy is examined and what action may be taken based on the examination.

Email filter profile configuration settings

The following are email filter profile configuration settings in *UTM Profiles > Email Filter > Profile*. Advanced settings are configured in the CLI.

Profile page Lists each individual email filter profile that you created. On this page, you can edit, delete or create a new email filter profile. You are redirected to this page when you select <i>View List</i> on the Edit Email Filter Profile page.	
Create New	Creates a new email filter profile. When you select <i>Create New</i> , you are automatically redirected to the New Email Filter Profile page.
Edit	Modifies settings within an email filtering profile. When you select <i>Edit</i> , you are automatically redirected to the Edit Email Filter Profile page.
Delete	Removes an email filter profile from the list. To remove multiple email filter profiles from within the list, on the Profile page, in each of the rows of the email filter profiles you want removed, select the check box and then select <i>Delete</i> . To remove all email filter profiles from the list, on the Profile page, select the check box in the check box column and then select <i>Delete</i> .

Name	The name of the email filter profile.
Comments	The description given to the email filter profile. This is an optional setting.
Ref.	<p>Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a firewall policy; on the Profile page (<i>UTM Profiles > Antivirus > Profile</i>), 1 appears in <i>Ref.</i>.</p> <p>To view the location of the referenced object, select the number in <i>Ref.</i>, and the Object Usage window appears displaying the various locations of the referenced object.</p> <p>To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:</p> <ul style="list-style-type: none"> • View the list page for these objects – automatically redirects you to the list page where the object is referenced at. • Edit this object – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • View the details for this object – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy, and that firewall policy's settings appear within the table.
<p>New Email Filter Profile page</p> <p>Provides settings for configuring multiple email filter profiles. If you are editing an email filter profile, you are automatically redirected to the Edit Email Filter Profile page.</p> <p>This page appears when you select <i>Create New</i> on the Edit Email Filter Profile page. If you are on the Profile page, and you select <i>Create New</i>, you will be redirected to the New Email Filter Profile page.</p> <p>Note: Logging is enabled in the CLI.</p>	
Name	<p>Enter a name for the email filter profile.</p> <p>If you are editing an existing email profile and want to change the name, enter the new name in the <i>Name</i> field and then select <i>Apply</i> to save the changes.</p>
Comments	<p>Enter a description about the email filter profile. This is optional.</p> <p>If you are editing an existing email profile and want to change the description, enter the new description in the <i>Comments</i> field and then select <i>Apply</i> to save the changes.</p>
Log Email Summary	<p>Select to log specific information about the spam email activity on protocols such as IMAP or web mail such as Yahoo Mail.</p> <p>This feature does not record all email filtering activity, only IMAP, POP3, SMTP, Yahoo Mail, and MSN Hotmail spam detected email messages. If you want to log all email filtering activity, you must enable it in the CLI.</p>

Enable Spam Detection and Filtering	Select to enable specific settings for detecting and filtering spam email messages for IMAP, POP3 and SMTP as well as IMAPS, POP3S and SMTPS.
Spam Action	<p>Select to either tag or discard email that the unit determines to be spam. Tagging adds the text in the <i>Tag Format</i> field to the subject line or header of an email message that is identified as spam. Discard is available only for SMTP.</p> <p>Note: When you enable virus scanning for SMTP and SMTPS in an antivirus profile, scanning in splice mode is also called streaming mode and is enabled automatically. When scanning in splice mode, the unit scans and streams the traffic to the destination at the same time, terminating the stream to the destination if a virus is selected.</p> <p>For more information about splicing behavior for SMTP, see the Knowledge Base article FortiGate Proxy Splice and Client Comforting Technical Note.</p> <p>When virus scanning is enabled for SMTP, the unit can only discard spam email if a virus is detected. Discarding immediately drops the connection. If virus scanning is not enabled, you can choose to either tag or discard SMTP spam.</p>
Tag Location	<p>Select to add the tag to the subject or MIME header of email identified as spam.</p> <p>If you select to add the tag to the subject line, the unit converts the entire subject line, including the tag, to UTF-8 format. This improves display for some email clients that cannot properly display subject lines that use more than one encoding.</p> <p>To add the tag to the MIME header, you must enable spamhdrcheck in the CLI for each protocol (IMAP, POP3 and SMTP).</p>
Tag Format	<p>Enter a word or phrase with which to tag email identified as spam. When typing a tag, use the same language as the unit's current administrator language setting. Tag text using other encodings may not be accepted. For example, when entering a spam tag that uses Japanese characters, first verify that the administrator language settings is Japanese; the unit will not accept a spam tag written in Japanese characters while the administrator language setting is English.</p> <p>Tags must not exceed 64 bytes. The number of characters constituting 64 bytes of data varies by text encoding, which may vary by the FortiGate administrator language setting.</p>

FortiGuard Spam Filtering	<p>Appears only when <i>Enable Spam Detection and Filtering</i> is enabled.</p> <p>Select to enable FortiGuard spam filtering.</p>
Local Spam Filtering	<p>Appears only when <i>Enable Spam Detection and Filtering</i> is enabled.</p> <p>Select to enable local spam filtering. Select the various check boxes beside the options you want included in the profile.</p> <p>When you enable local spam filtering, you can apply email address and IP address black and white lists, as well as a banned word list to the profile.</p>

Banned Word

Control spam by blocking email messages containing specific words or patterns. You can add words, phrases, wild cards and Perl regular expressions to match content in email messages. For information, about wild cards and Perl regular expressions, see [“Using wildcards and Perl regular expressions” on page 281](#).

The unit checks each email message against the banned word list. The unit can sort email messages containing those banned words in the subject, body, or both. The score value of each banned word appearing in the message is added, and if the total is greater than the threshold value set in the email filter profile, the unit processes the message according to the setting in the profile. The score for a pattern is applied only once even if the word appears in the message multiple times.

Banned word configuration settings

The following are banned word configuration settings in *UTM Profiles > Email Filter > Banned Word*.

Banned Word page	
Lists each banned word list that you created. On this page you can edit, delete or create a new banned word.	
Create New	Creates a new banned word. When you select <i>Create New</i> , you are automatically redirected to the New List page. This page provides a name field and comment field. You must enter a name to go to the Banned Word Settings page.
Edit	Modifies the banned word list, list name, or list comment. When you select <i>Edit</i> , you are automatically redirected to the Banned Word Settings page.
Delete	<p>Removes the banned word list from the catalog. The <i>Delete</i> icon is available only if the banned word list is not selected in any email filter profiles.</p> <p>To remove multiple banned word lists from within the list, on the Banned Word page, in each of the rows of the banned word lists you want removed, select the check box and then select <i>Delete</i>.</p> <p>To remove all banned word lists from the list, on the Banned Word page, select the check box in the check box column and then select <i>Delete</i>.</p>
Name	The available Email Filter banned word lists.
# Entries	The number of entries in each banned word list.
Comments	Optional description of each banned word list.
Ref.	<p>Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a firewall policy; on the Profile page (<i>UTM Profiles > Antivirus > Profile</i>), 1 appears in <i>Ref.</i>.</p> <p>To view the location of the referenced object, select the number in <i>Ref.</i>, and the Object Usage window appears displaying the various locations of the referenced object.</p> <p>To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:</p> <ul style="list-style-type: none"> • View the list page for these objects – automatically redirects you to the list page where the object is referenced at. • Edit this object – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • View the details for this object – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy, and that firewall policy's settings appear within the table.

Banned Word Settings page	
Provides settings for configuring a word pattern or word that will be considered banned by the unit. These words and word patterns make up a banned word list which appears on the Banned Word page. If you are editing a banned word, you are automatically redirected to the Banned Word Settings page.	
Name	If you are editing an existing banned word list and you want to change the name, enter a new name in this field. You must select <i>OK</i> to save these changes.
Comments	If you are editing an existing banned word list and want to change or add a description, enter the new text in this field. You must select <i>OK</i> to save these changes.
Create New	Adds a word or phrase to the banned word list. When you select <i>Create New</i> , you are automatically redirected to the Add Banned Word page.
Edit	Modifies banned word settings. When you select <i>Edit</i> , you are automatically redirected to the Edit Banned Word page.
Delete	Removes a banned word from the list. To remove multiple banned words from within the list, on the Banned Word Settings page, in each of the rows of the words you want removed, select the check box and then select <i>Delete</i> . To remove all banned words from the list, on the Banned Word Settings page, select the check box in the check box column and then select <i>Delete</i> .
Enable	Enables a banned word within the list.
Disable	Disables a banned word within the list.
Remove All Entries	Removes all banned word entries within the list on the Banned Word Settings page.
Page Controls	Use to navigate through the information in the Banned Word menu.
Enable	A green checkmark appears if the banned word is enabled.
Pattern	The list of banned words. Select the check box to enable all the banned words in the list.
Pattern Type	The pattern type used in the banned word list entry. Choose from wildcard or regular expression. For more information, see “Using wildcards and Perl regular expressions” on page 281 .
Language	The character set to which the banned word belongs.
Where	The location where the unit searches for the banned word: <i>Subject</i> , <i>Body</i> , or <i>All</i> .
Score	A numerical weighting applied to the banned word. The score values of all the matching words appearing in an email message are added, and if the total is greater than the Banned word check value set in the profile, the email is processed according to whether the spam action is set to <i>Discard</i> or <i>Tagged</i> in the email filter profile. The score for a banned word is counted once even if the word appears multiple times on the web page in the email. For more information, see “Email Filter interface reference” on page 64 .

Add Banned Word page	
Provides settings for configuring a banned word entry.	
Pattern	<p>Enter the banned word pattern.</p> <p>A pattern can be part of a word, a whole word, or a phrase. Multiple words entered as a pattern are treated as a phrase. The phrase must appear exactly as entered to match. You can also use wildcards or regular expressions to have a pattern match multiple words or phrases.</p>
Pattern Type	Select the pattern type for the banned word. Choose from wildcard or regular expressions. For more information, see “Using wildcards and Perl regular expressions” on page 281 .
Language	Select the character sets for the banned word.
Where	Select where the Fortinet unit should search for the banned word, <i>Subject</i> , <i>Body</i> , or <i>All</i> .
Score	<p>Enter a score for the pattern.</p> <p>Each entry in the banned word list added to the profile includes a score. When an email message is matched with an entry in the banned word list, the score is recorded. If an email message matches more than one entry, the score for the email message increases. When the total score for an email message equals or exceeds the threshold, the message is considered spam and handled according to the spam action configured in the profile.</p>
Enable	Select to enable a disable banned word. By default, a banned word is enabled.



Perl regular expression patterns are case sensitive for banned words. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` will block all instances of `bad language` regardless of case. Wildcard patterns are not case sensitive.

IP Address

You can add IP address black/white lists and email address black/white lists to filter email. When performing an IP address list check, the unit compares the IP address of the message sender to the IP address list items in sequence. When performing an email list check, the unit compares the email address of the message sender to the email address list items in sequence. If a match is found, the action associated with the IP address or email address is taken. If no match is found, the message is passed to the next enabled email filter.

You can add multiple IP address lists and then select the best one for each email filter profile.

After creating an IP address list, you can add IP addresses to the list.

Enter an IP address or a pair of IP address and mask in the following formats:

- `x.x.x.x`, for example, 192.168.69.100.
- `x.x.x.x/x.x.x.x`, for example, 192.168.69.100/255.255.255.0
- `x.x.x.x/x`, for example, 192.168.69.100/24

IP address configuration settings

The following are IP address configuration settings in *UTM Profiles > Email Filter > IP Address*.

IP Address page Lists each individual IP address list that you created. On this page, you can edit, delete or create a new IP address list. An IP address list contains multiple IP addresses and this list is configured in the IP Address Settings page.	
Create New	Creates a new IP address list. When you select <i>Create New</i> , you are automatically redirected to the New List page. This page provides a name field and comment field. You must enter a name to go to the IPS Address Settings page.
Edit	Modifies settings within an IP address list. When you select <i>Edit</i> , you are automatically redirected to the IP Address Settings page.
Delete	<p>Removes the IP address black/white list from the list. The <i>Delete</i> icon is available only if the IP address list is not selected in any profiles.</p> <p>To remove multiple IP address black/white lists from within the list, on the IP Address page, in each of the rows of the black/white lists you want removed, select the check box and then select <i>Delete</i>.</p> <p>To remove all IP address lists from the list, on the IP Address page, select the check box in the check box column and then select <i>Delete</i>.</p>
Name	The available name of the IP address lists.
# Entries	The number of entries in each IP address list.
Comments	Optional description of each IP address list.

Ref.	<p>Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a firewall policy; on the Profile page (<i>UTM Profiles > Antivirus > Profile</i>), 1 appears in <i>Ref.</i></p> <p>To view the location of the referenced object, select the number in <i>Ref.</i>, and the Object Usage window appears displaying the various locations of the referenced object.</p> <p>To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:</p> <ul style="list-style-type: none"> • View the list page for these objects – automatically redirects you to the list page where the object is referenced at. • Edit this object – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • View the details for this object – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy, and that firewall policy's settings appear within the table.
IP Address Settings page Provides settings for configuring multiple IP addresses that are then grouped together to form a list of IP addresses. This list is then applied within the email filter profile. You are automatically redirected to this page from the New List page. If you are editing an IP Address, you are automatically redirected to the IP Address Settings page.	
Name	If you are editing an existing IP address list and want to change the name, enter a new name in this field. You must select <i>OK</i> to save the change.
Comments	If you are editing an existing IP address list and want to change or add a description, enter the new text in this field. You must select <i>OK</i> to save the changes.
Create New	Creates a new IP address with settings. When you select <i>Create New</i> , you are automatically redirected to the Add IP Address page.
Edit	Modifies the settings within an IP address. When you select <i>Edit</i> , you are automatically redirected to the Edit IP Address page.

Delete	<p>Removes an IP address from the list.</p> <p>To remove multiple IP addresses from within the list, on the IP Address Settings page, in each of the rows of the IP addresses you want removed, select the check box and then select <i>Delete</i>.</p> <p>To remove all IP addresses from the list, on the IP Address Settings page, select the check box in the check box column and then select <i>Delete</i>.</p>
Enable	Enables an IP address within that IP address list.
Disable	Disables an IP address within that IP address list.
Move To	<p>Moves the entry to a different position in the list. When you select <i>Move To</i>, the Move IP Address window appears.</p> <p>To move an IP address, select the new position <i>Before</i> or <i>After</i>, which will place the current IP address before or after the IP address you enter in the field (<i>IP/Netmask</i>). Enter the IP address and netmask in the (<i>IP/Netmask</i>) field.</p> <p>The firewall policy executes the list from top to bottom. For example, if you have IP address 192.168.100.1 listed as spam and 192.168.100.2 listed as clear, you must put 192.168.100.1 above 192.168.100.2 for 192.168.100.1 to take effect.</p>
Remove All Entries	Removes all IP addresses from within the list on the IP Address Settings page.
Enable	Indicates that the IP address is either enabled or disabled. A green check mark indicates that it is enabled; a gray x indicates that it is disabled.
IP/Netmask	The IP address and/or netmask.
Action	The type of action the unit will take when a match is detected. For example, the <i>Action</i> is <i>Spam</i> ; when a match is found, the detected IP address is considered spam.
Add IP Address page	
Provides settings for configuring an IP address to add to the list.	
IP/Netmask	Enter the IP address or the IP address/mask pair.
Action	Select: <i>Mark as Spam</i> to apply the spam action configured in the profile, <i>Mark as Clear</i> to bypass this and remaining email filters, or <i>Mark as Reject</i> (SMTP or SMTPS) to drop the session.
Enable	Select to enable the address.

E-mail Address

The unit can filter email from specific senders or all email from a domain (such as example.net). You can add email address lists and then select the best one for each profile.

Email address configuration settings

The following are email address configuration settings in *UTM Profiles > Email Filter > E-mail Address*.

E-mail Address page	
Lists each individual email address list that you created. On this page, you can edit, delete or create a new email address list.	
Create New	Creates a new email address list. When you select <i>Create New</i> , you are automatically redirected to the New List page. This page provides a name field and comment field; you must enter a name to go to the E-mail Address Settings page.
Edit	Modifies settings within an email address list. When you select <i>Edit</i> , you are automatically redirected to the E-mail Address Settings page.
Delete	Removes the email address list from the list on the E-mail Address page. The <i>Delete</i> icon is only available if the email address list is not selected in any profiles. To remove multiple email address lists from within the list, on the E-mail Address page, in each of the rows of the lists you want removed, select the check box and then select <i>Delete</i> . To remove all email filter lists from the list, on the E-mail Address page, select the check box in the check box column and then select <i>Delete</i> .
Name	The name of the email address list.
# Entries	The number of entries in each email address list.
Comments	Optional description of each email address list.

Ref.	<p>Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a firewall policy; on the Profile page (<i>UTM Profiles > Antivirus > Profile</i>), 1 appears in <i>Ref.</i>.</p> <p>To view the location of the referenced object, select the number in <i>Ref.</i>, and the Object Usage window appears displaying the various locations of the referenced object.</p> <p>To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:</p> <ul style="list-style-type: none"> • View the list page for these objects – automatically redirects you to the list page where the object is referenced at. • Edit this object – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • View the details for this object – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy, and that firewall policy's settings appear within the table.
E-mail Address Settings page Provides settings for configuring multiple email addresses that are then grouped together to form a list of email addresses. This list is then applied within the email filter profile. You are automatically redirected to this page from the New List page. If you are editing an email address list, you are automatically redirected to the E-mail Address Settings page.	
Name	If you are editing an existing email address list and want to change the name, enter a new name in this field. You must select <i>OK</i> to save the change.
Comments	If you are editing an existing email address list and want to change or add a description, enter the new text in this field. You must select <i>OK</i> to save the changes.
Create New	Creates a new email address to the email address list. When you select <i>Create New</i> , you are automatically redirected to the Add E-mail Address page.
Edit	Modifies settings within that email address in the list on the E-mail Address Settings page. When you select <i>Edit</i> , you are automatically redirected to the Edit E-mail Address page.
Delete	Removes an email address from within the list on the E-mail Address Settings page.
Enable	Enables an email address within the list.
Disable	Disables an email address within the list.

Move To	Moves the entry to a different position in the list. When you select <i>Move To</i> , the Move E-mail Address window appears. To move an email address, select the new position <i>Before</i> or <i>After</i> , which will place the current email address before or after the email address you enter in the (<i>E-mail Address</i>) field. Enter the email address in the field and then select <i>OK</i> .
Remove All Entries	Removes all email addresses within the list on the E-mail Address Settings page.
Page Controls	Use to navigate through the lists on the E-mail Address Settings page.
Enable	A green checkmark appears if an email address is enabled. A gray x appears if an email address is disabled.
E-mail Address	The email address entered.
Pattern Type	The pattern type chosen for that email address.
Action	The action that will be take when that email address is detected.
Add E-Mail Address page	
E-mail Address	Enter the email address.
Pattern Type	Select a pattern type: <i>Wildcard</i> or <i>Regular Expression</i> . For more information, see “Using wildcards and Perl regular expressions” on page 281 .
Action	Select: <i>Mark as Spam</i> to apply the spam action configured in the profile, or <i>Mark as Clear</i> to bypass this and remaining email filters.
Enable	Select to enable the email address.



Intrusion protection

The FortiGate Intrusion Protection system combines signature detection and prevention with low latency and excellent reliability. With intrusion protection, you can create multiple IPS sensors, each containing a complete configuration based on signatures. Then, you can apply any IPS sensor to any security policy.

This section describes how to configure the FortiGate Intrusion Protection settings.

If you enable virtual domains (VDOMs) on the FortiGate unit, intrusion protection is configured separately for each virtual domain.

The following topics are included:

- [IPS concepts](#)
- [Enable IPS scanning](#)
- [Configure IPS options](#)
- [Enable IPS packet logging](#)
- [IPS examples](#)

IPS concepts

The FortiGate intrusion protection system protects your network from outside attacks. Your FortiGate unit has two techniques to deal with these attacks: anomaly- and signature-based defense.

Anomaly-based defense

Anomaly-based defense is used when network traffic itself is used as a weapon. A host can be flooded with far more traffic than it can handle, making the host inaccessible. The most common example is the denial of service (DoS) attack, in which an attacker directs a large number of computers to attempt normal access of the target system. If enough access attempts are made, the target is overwhelmed and unable to service genuine users. The attacker does not gain access to the target system, but it is not accessible to anyone else.

The FortiGate DoS feature will block traffic above a certain threshold from the attacker and allow connections from other legitimate users.

Signature-based defense

Signature-based defense is used against known attacks or vulnerability exploits. These often involve an attacker attempting to gain access to your network. The attacker must communicate with the host in an attempt to gain access and this communication will include particular commands or sequences of commands and variables. The IPS signatures include these command sequences, allowing the FortiGate unit to detect and stop the attack.

Signatures

IPS signatures are the basis of signature-based intrusion protection. Every attack can be reduced to a particular string of commands or a sequence of commands and variables. Signatures include this information so your FortiGate unit knows what to look for in network traffic.

Signatures also include characteristics about the attack they describe. These characteristics include the network protocol in which the attack will appear, the vulnerable operating system, and the vulnerable application.

To view the complete list of predefined signatures, go to *UTM Profiles > Intrusion Protection > Predefined*.

IPS engine

The IPS engine examines the network traffic for the attack signatures.

IPS sensors

The IPS engine does not examine network traffic for all signatures, however. You must first create an IPS sensor and specify which signatures are included. Add signatures to sensors individually using signature entries, or in groups using IPS filters.

To view the IPS sensors, go to *UTM Profiles > Intrusion Protection > IPS Sensor*.

IPS filters

IPS sensors contain one or more IPS filters. A filter can be a collection of signature attributes that you specify. The signatures that have all of the attributes specified in a filter are included in the IPS filter. Another option is to configure a filter with a list of signatures that you choose.

For example, if your FortiGate unit protects a Linux server running the Apache web server software, you could create a new filter to protect it. By setting *OS* to *Linux*, and *Application* to *Apache*, the filter will include only the signatures that apply to both Linux and Apache. If you wanted to scan for all the Linux signatures and all the Apache signatures, you would create two filters, one for each.

To view the filters in an IPS sensor, go to *UTM Profiles > Intrusion Protection > IPS Sensor*, select the IPS sensor containing the filters you want to view, and choose *Edit*.

Adding custom/predefined signatures

IPS filters can be configured to allow you to add an individual custom or predefined IPS signatures. If you need only one signature, this is the easiest way. Signature-mode IPS filters are also the only way to include custom signatures in an IPS sensor.

Another use for signature-mode filters are to change the settings of individual signatures that are already included in a filter within the same IPS sensor. Add a signature-mode filter with the required settings above the regular filter, and the signature-mode filter will take priority.

Policies

To use an IPS sensor, you must select it in a security policy or an interface policy. An IPS sensor that is not selected in a policy will have no effect on network traffic.

IPS is most often configured as part of a security policy. Unless stated otherwise, discussion of IPS sensor use will be in regards to firewall policies in this document.

Enable IPS scanning

Enabling IPS scanning involves two separate parts of the FortiGate unit:

- The security policy allows certain network traffic based on the sender, receiver, interface, traffic type, and time of day. Firewall policies can also be used to deny traffic, but those policies do not apply to IPS scanning.
- The IPS sensor contains filters, signature entries, or both. These specify which signatures are included in the IPS sensor.

When IPS is enabled, an IPS sensor is selected in a security policy, and all network traffic matching the policy will be checked for the signatures in the IPS sensor.

General configuration steps

For best results in configuring IPS scanning, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

- 1 Create an IPS sensor.
- 2 Add filters one or more filters to the sensor. The filters specify which signatures the IPS engine will look for in the network traffic.
- 3 Select a security policy or create a new one.
- 4 In the security policy, enable UTM protection, select *Enable IPS*, and choose the IPS sensor from the list.

All the network traffic controlled by this security policy will be processed according to the settings in the policy. These settings include the IPS sensor you specify in the policy.

Creating an IPS sensor

You need to create an IPS sensor and save it before configuring it with filters and entries.

To create a new IPS sensor

- 1 Go to *UTM Profiles > Intrusion Protection > IPS Sensor*.
- 2 Select the *Create New* icon in the top of the Edit IPS Sensor window.
- 3 Enter the name of the new IPS sensor.
- 4 Optionally, you may also enter a comment. The comment will appear in the IPS sensor list and serves to remind you of the details of the sensor.
- 5 Select *OK*.

The IPS sensor is created and the sensor configuration window appears. A newly created sensor is empty and contains no filters or signatures. You need to add one or more filters or signatures before the sensor can take effect.

Creating an IPS filter

While individual signatures can be added to a sensor, a filter allows you to add multiple signatures to a sensor by specifying the characteristics of the signatures to be added.

To create a new IPS filter

- 1 Go to *UTM Profiles > Intrusion Protection > IPS Sensor*.
- 2 Select the IPS sensor to which you want to add the filter using the drop-down list in the top row of the Edit IPS Sensor window.
- 3 Select the *Create New* drop-down and choose *Filter*.

- 4 Configure the filter that you require. Signatures matching all of the characteristics you specify in the filter will be included in the filter.

Type	Select the type of IPS filter to create.
Filter	A filter-mode IPS filter allows you to select a number of filter attributes. The signatures that match all the selected attributes are included in the filter.
Signature	A signature-mode IPS filter allows you to select the specific filters, by name, that are included in the filter.
Pre-defined Signatures	Select Add to choose a predefined signature to include in the IPS filter. You can add as many signatures as you require, but if need a large number, consider using the filter type.
Custom Signatures	Select Add to choose a custom signature to include in the IPS filter.
Severity	Select <i>Specify</i> and choose the severity levels to include in the filter. If you select <i>All</i> , the severity attribute will not be used to determine which signatures are included in the filter.
Target	Select <i>Specify</i> and choose the type of system the signature protects. If you select <i>All</i> , the target attribute will not be used to determine which signatures are included in the filter.
OS	Select <i>Specify</i> and choose the operating system the signature protects. If you select <i>All</i> , the OS attribute will not be used to determine which signatures are included in the filter. Predefined signatures listed with an OS attribute of <i>All</i> affect all operating system and are automatically included in any filter regardless of whether a single, multiple, or all operating systems are specified.
Protocol	Select <i>Specify</i> and choose the network protocols the signature protects by selecting an item in the Available column and using the right-arrow icon to move the item to the Selected column. Similarly, remove protocols by selecting an item in the Selected column and use the left-arrow icon to move the item to the Available column. If you select <i>All</i> , the Protocol attribute will not be used to determine which signatures are included in the filter.

Application	<p>Select <i>Specify</i> and choose the applications the signature protects by selecting an item in the Available column and using the right-arrow icon to move the item to the Selected column.</p> <p>Similarly, remove applications by selecting an item in the Selected column and using the left-arrow icon to move the item to the Available column.</p> <p>If you select <i>All</i>, the Application attribute will not be used to determine which signatures are included in the filter.</p>
Tags	<p>Tags are a means by which you can apply customized labels to your IPS filters. Specified tags are displayed only within the filter itself on the Edit IPS Filter page.</p> <p>By default, the tag feature is disabled on all but the largest FortiGate models. If the Tags option is not visible, you must go to <i>System > Admin > Settings</i> and enable <i>Display Object Tagging and Coloring</i> to enable it.</p> <p>For more information about tags, see the System Administration Guide.</p>
Applied Tags	Displays the tags that you have applied to the filter.
Add tags	Enter a tag and then select the plus (+) icon to add the tag to the filter. This also adds the tag to the <i>Applied tags</i> list.
View Matched rules	Select view a list of all the signatures included in the filter with the current settings.
Action	<p>All predefined signatures have an <i>Action</i> attribute that is set to Pass or Drop. Select <i>Accept signature defaults</i> use the default action for each included signature. This means that if a signature included in the filter has an <i>Action</i> setting of Pass, traffic matching the signature will be detected and then allowed to continue to its destination.</p> <p>Select <i>Monitor all</i> to pass all traffic matching the signatures included in the filter, regardless of their default <i>Action</i> setting. Similarly, you may select <i>Block all</i> to drop traffic matching any the signatures included in the filter. Select <i>Reset</i> to reset the connection when a matching signature is detected.</p>
Action	<p>All predefined signatures have an <i>Enable</i> attribute that is set to on or off. Select <i>Accept signature defaults</i> use the <i>Enable</i> default setting for each included signature. This means that if a signature included in the filter has an <i>Enable</i> setting of off, traffic matching the signature will not be detected even though the signature is included in the filter.</p> <p>Select <i>Enable all</i> to enable all the signatures included in the filter, regardless of their <i>Enable</i> setting. Similarly, you may select <i>Disable all</i> to disable all the signatures included in the filter.</p>

Packet Logging	<p>Select to enable packet logging for the filter.</p> <p>When you enable packet logging on a filter, the unit saves a copy of the packets that match any signatures included in the filter. The packets can be analyzed later.</p> <p>For more information about packet filtering, see “Viewing and saving logged packets” on page 280</p>
Quarantine Attackers (to Banned Users List)	<p>Enable this option to add the source of the offending traffic to the Banned User list. When enabled, select the method and the expiry time.</p>

5 Select OK.

The filter is created and added to the filter list.

Filter order

Each time a FortiGate unit receives traffic passing through one of its interfaces, the unit checks the security policy that allowed the traffic for its IPS configuration. If IPS is enabled, the FortiGate unit examines the specified sensor and checks the traffic for the signatures in the first filter. If there's no match, it checks for the signatures in the second filter, and so on until a match is found or all the filters yield no matches. If there are no matches, the traffic is allowed. If there is a match, further checking for matching IPS signatures is stopped and the configured action is applied. Because further checking is stopped, the sequence of the filters is important.

For example, take a sensor in which there are two filters. One that includes all the signatures with a monitor action, and a second with a single filter configured to block an individual signature. If the 'all signature' filter is first, the second filter will never be triggered since the same filter is included in the first, and configure to monitor. Traffic that triggers the signature will never be blocked. In this case, the first filter acts as a signature override.

If the 'all signature' filter is second, traffic matching the individual signature will be detected and blocked before reaching the second filter. All other non-matching traffic will be checked for matches in the second filter.

Generally, as in this example, filters should be arranged from the specific to the general, with custom signatures at the very top of the list.

Updating predefined IPS signatures

The FortiGuard Service periodically updates the pre-defined signatures and adds new signatures to counter emerging threats as they appear.

Because the signatures included in filters are defined by specifying signature attributes, new signatures matching existing filter specifications will automatically be included in those filters. For example, if you have a filter that includes all signatures for the Windows operating system, your filter will automatically incorporate new Windows signatures as they are added.

Viewing and searching predefined IPS signatures

Go to *UTM Profiles > Intrusion Protection > Predefined* to view the list of predefined IPS signatures. You may find signatures by paging manually through the list, apply filters, or by using the search field.

Searching manually

Signatures are displayed in a paged list, with 50 signatures per page. The bottom of the screen shows the current page and the total number of pages. You can enter a page number and press enter, to skip directly to that page. Previous Page and Next Page buttons move you through the list, one page at a time. The First Page and Last Page button take you to the beginning or end of the list.

Applying filters

You can enter criteria for one of more columns, and only the signatures matching all the conditions you specify will be listed.

To apply filters

- 1 Go to *UTM Profiles > Intrusion Protection > Predefined*.
- 2 Select Filter Settings.
- 3 Select Add New Filter.
- 4 Select column by which to filter.
- 5 Select the item or items by which to filter.
- 6 Continue to add more filters to narrow your search, if required.
- 7 Select OK.

The available options vary by column. For example, Enable allows you to choose between two options, while OS has multiple options, and you may select multiple items together. Filtering by name allows you to enter a text string and all signature names containing the string will be displayed.

Using the search field

To use the search field, located above the signature list, start typing any portion of the signature name. Signatures names matching the text you enter are displayed in a drop-down list. A maximum of ten matches are displayed at a time.

Select a signature from the drop-down list to display its signature list entry.

Creating a custom IPS signature

The FortiGate predefined signatures cover common attacks. If you use an unusual or specialized application or an uncommon platform, add custom signatures based on the security alerts released by the application and platform vendors.

You can add or edit custom signatures using the web-based manager or the CLI.

To create a custom signature

- 1 Go to *UTM Profiles > Intrusion Protection > Custom*.
- 2 Select *Create New* to add a new custom signature.
- 3 Enter a *Name* for the custom signature.
- 4 Enter the *Signature*. For information about completing this field, see [“Custom signature syntax and keywords”](#).
- 5 Select OK.

Custom signature syntax and keywords

All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. The syntax and keywords are detailed in the next two topics.

Custom signature syntax

A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.

A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [()]. The keyword and value pairs are separated by a semi colon (;) and consist of a keyword and a value separated by a space. The basic format of a definition is HEADER (KEYWORD VALUE;)

You can use as many keyword/value pairs as required within the 512 character limit. To configure a custom signature, go to *UTM Profiles > Intrusion Protection > Custom* and enter the data directly into the *Signature* field, following the guidance in the next topics.

[Table 2](#) shows the valid characters and basic structure. For details about each keyword and its associated values, see [“Custom signature keywords” on page 87](#).

Table 2: Valid syntax for custom signature fields

Field	Valid Characters	Usage
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.
KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See “Custom signature keywords” on page 87 for tables of supported keywords.
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.

Custom signature keywords

Table 3: Information keywords

Keyword and value	Description
<code>--attack_id <id_int>;</code>	<p>Use this optional value to identify the signature. It cannot be the same value as any other custom rules. If an attack ID is not specified, the FortiGate automatically assigns an attack ID to the signature. If you are using VDOMs, custom signatures appear only in the VDOM in which you create them. You can use the same attack ID for signatures in different VDOMs.</p> <p>An attack ID you assign must be between 1000 and 9999.</p> <p>Example:</p> <pre>--attack_id 1234;</pre>
<code>--name <name_str>;</code>	<p>Enter the name of the rule. A rule name must be unique. If you are using VDOMs, custom signatures appear only in the VDOM in which you create them. You can use the same rule name for signatures in different VDOMs.</p> <p>The name you assign must be a string greater than 0 and less than 64 characters in length.</p> <p>Example:</p> <pre>--name "Buffer_Overflow";</pre>

Table 4: Session keywords

Keyword and value	Description
<code>--flow {from_client[,reversed] from_server[,reversed] bi_direction };</code>	<p>Specify the traffic direction and state to be inspected. They can be used for all IP traffic.</p> <p>Example:</p> <pre>--src_port 41523; --flow bi_direction;</pre> <p>The signature checks traffic to and from port 41523.</p> <p>If you enable “quarantine attacker”, the optional <code>reversed</code> keyword allows you to change the side of the connection to be quarantined when the signature is detected.</p> <p>For example, a custom signature written to detect a brute-force log in attack is triggered when “Login Failed” is detected <code>from_server</code> more than 10 times in 5 seconds. If the attacker is quarantined, it is the server that is quarantined in this instance. Adding <code>reversed</code> corrects this problem and quarantines the actual attacker.</p> <p>Previous FortiOS versions used <code>to_client</code> and <code>to_server</code> values. These are now deprecated, but still function for backwards compatibility.</p>

Table 4: Session keywords

<pre>--service {HTTP TELNET FTP DNS SMTP POP3 IMAP SNMP RADIUS LDAP MSSQL RPC SIP H323 NBSS DCERPC SSH SSL};</pre>	<p>Specify the protocol type to be inspected.</p> <p>This keyword allows you to specify the traffic type by protocol rather than by port. If the decoder has the capability to identify the protocol on any port, the signature can be used to detect the attack no matter what port the service is running on. Currently, HTTP, SIP, SSL, and SSH protocols can be identified on any port based on the content.</p>
--	--

Table 5: Content keywords

Keyword and value	Description
<pre>--byte_jump <bytes_to_convert>, <offset>[, relative] [, big] [, little] [, string] [, hex] [, dec] [, oct] [, align];</pre>	<p>Use the <code>byte_jump</code> option to extract a number of bytes from a packet, convert them to their numeric representation, and jump the match reference up that many bytes (for further pattern matching or byte testing). This keyword allows relative pattern matches to take into account numerical values found in network data.</p> <p>The available keyword options include:</p> <ul style="list-style-type: none"> • <code><bytes_to_convert></code>: The number of bytes to examine from the packet. • <code><offset></code>: The number of bytes into the payload to start processing. • <code>relative</code>: Use an offset relative to last pattern match. • <code>big</code>: Process the data as big endian (default). • <code>little</code>: Process the data as little endian. • <code>string</code>: The data is a string in the packet. • <code>hex</code>: The converted string data is represented in hexadecimal notation. • <code>dec</code>: The converted string data is represented in decimal notation. • <code>oct</code>: The converted string data is represented in octal notation. • <code>align</code>: Round up the number of converted bytes to the next 32-bit boundary.

Table 5: Content keywords (Continued)

Keyword and value	Description
<pre>--byte_test <bytes_to_convert>, <operator>, <value>, <offset>[, relative] [, big] [, little] [, string] [, hex] [, dec] [, oct];</pre>	<p>Use the <code>byte_test</code> keyword to compare a byte field against a specific value (with operator). This keyword is capable of testing binary values or converting representative byte strings to their binary equivalent and testing them.</p> <p>The available keyword options include:</p> <ul style="list-style-type: none"> • <code><bytes_to_convert></code>: The number of bytes to compare. • <code><operator></code>: The operation to perform when comparing the value (<, >, =, !=, &). • <code><value></code>: The value to compare the converted value against. • <code><offset></code>: The number of bytes into the payload to start processing. • <code>relative</code>: Use an offset relative to last pattern match. • <code>big</code>: Process the data as big endian (default). • <code>little</code>: Process the data as little endian. • <code>string</code>: The data is a string in the packet. • <code>hex</code>: The converted string data is represented in hexadecimal notation. • <code>dec</code>: The converted string data is represented in decimal notation. • <code>oct</code>: The converted string data is represented in octal notation.
<pre>--depth <depth_int>;</pre>	<p>Use the <code>depth</code> keyword to search for the contents within the specified number of bytes after the starting point defined by the <code>offset</code> keyword. If no <code>offset</code> is specified, the <code>offset</code> is assumed to be equal to 0.</p> <p>If the value of the <code>depth</code> keyword is smaller than the length of the value of the <code>content</code> keyword, this signature will never be matched.</p> <p>The <code>depth</code> must be between 0 and 65535.</p>
<pre>--distance <dist_int>;</pre>	<p>Use the <code>distance</code> keyword to search for the contents within the specified number of bytes relative to the end of the previously matched contents. If the <code>within</code> keyword is not specified, continue looking for a match until the end of the payload.</p> <p>The <code>distance</code> must be between 0 and 65535.</p>

Table 5: Content keywords (Continued)

Keyword and value	Description
<pre>--content [!]"<content_str>;</pre>	<p>Deprecated, see <code>pattern</code> and <code>context</code> keywords.</p> <p>Use the <code>content</code> keyword to search for the content string in the packet payload. The content string must be enclosed in double quotes.</p> <p>To have the FortiGate search for a packet that does not contain the specified context string, add an exclamation mark (!) before the content string.</p> <p>Multiple content items can be specified in one rule. The value can contain mixed text and binary data. The binary data is generally enclosed within the pipe () character.</p> <p>The double quote ("), pipe sign() and colon(:) characters must be escaped using a back slash if specified in a content string.</p> <p>If the value of the <code>content</code> keyword is greater than the length of the value of the <code>depth</code> keyword, this signature will never be matched.</p>
<pre>--context {uri header body host};</pre>	<p>Specify the protocol field to look for the pattern. If context is not specified for a pattern, the FortiGate unit searches for the pattern anywhere in the packet buffer. The available context variables are:</p> <ul style="list-style-type: none"> • <code>uri</code>: Search for the pattern in the HTTP URI line. • <code>header</code>: Search for the pattern in HTTP header lines or SMTP/POP3/SMTP control messages. • <code>body</code>: Search for the pattern in HTTP body or SMTP/POP3/SMTP email body. • <code>host</code>: Search for the pattern in HTTP HOST line. <p>Example:</p> <pre>--pattern "GET " --context uri --pattern "yahoo.com" --context host --no_case --pcre "/DESCRIBE\s+\/\s+RTSP\/\s+i" --context header</pre>
<pre>--no_case;</pre>	<p>Use the <code>no-case</code> keyword to force the FortiGate unit to perform a case-insensitive pattern match.</p>

Table 5: Content keywords (Continued)

Keyword and value	Description
<code>--offset <offset_int>;</code>	<p>Use the <code>offset</code> keyword to look for the contents after the specified number of bytes into the payload. The specified number of bytes is an absolute value in the payload. Follow the <code>offset</code> keyword with the <code>depth</code> keyword to stop looking for a match after a specified number of bytes. If no <code>depth</code> is specified, the FortiGate unit continues looking for a match until the end of the payload.</p> <p>The <code>offset</code> must be between 0 and 65535.</p>
<code>--pattern [!]"<pattern_str>;</code>	<p>The FortiGate unit will search for the specified pattern.</p> <p>A <code>pattern</code> keyword normally is followed by a <code>context</code> keyword to define where to look for the pattern in the packet. If a <code>context</code> keyword is not present, the FortiGate unit looks for the pattern anywhere in the packet buffer.</p> <p>To have the FortiGate search for a packet that does not contain the specified URI, add an exclamation mark (!) before the URI.</p> <p>Example:</p> <pre>--pattern "/level/" --pattern " E8 D9FF FFFF /bin/sh" --pattern "! 20 RTSP/"</pre>

Table 5: Content keywords (Continued)

Keyword and value	Description
<pre>--pcre [!]"(/<regex>/ m<delim> <regex><delim>)[ismxAEG RUB]";</pre>	<p>Similarly to the <code>pattern</code> keyword, use the <code>pcre</code> keyword to specify a pattern using Perl-compatible regular expressions (PCRE). A <code>pcre</code> keyword can be followed by a <code>context</code> keyword to define where to look for the pattern in the packet. If no <code>context</code> keyword is present, the FortiGate unit looks for the pattern anywhere in the packet buffer.</p> <p>For more information about PCRE syntax, go to http://www.pcre.org.</p> <p>The switches include:</p> <ul style="list-style-type: none"> • <code>i</code>: Case insensitive. • <code>s</code>: Include newlines in the dot metacharacter. • <code>m</code>: By default, the string is treated as one big line of characters. <code>^</code> and <code>\$</code> match at the beginning and ending of the string. When <code>m</code> is set, <code>^</code> and <code>\$</code> match immediately following or immediately before any newline in the buffer, as well as the very start and very end of the buffer. • <code>x</code>: White space data characters in the pattern are ignored except when escaped or inside a character class. • <code>A</code>: The pattern must match only at the start of the buffer (same as <code>^</code>). • <code>E</code>: Set <code>\$</code> to match only at the end of the subject string. Without <code>E</code>, <code>\$</code> also matches immediately before the final character if it is a newline (but not before any other newlines). • <code>G</code>: Invert the “greediness” of the quantifiers so that they are not greedy by default, but become greedy if followed by <code>?</code>. • <code>R</code>: Match relative to the end of the last pattern match. (Similar to <code>distance:0</code>). • <code>U</code>: Deprecated, see the <code>context</code> keyword. Match the decoded URI buffers.

Table 5: Content keywords (Continued)

Keyword and value	Description
<code>--uri [!]"<uri_str>;</code>	<p>Deprecated, see <code>pattern</code> and <code>context</code> keywords.</p> <p>Use the <code>uri</code> keyword to search for the URI in the packet payload. The URI must be enclosed in double quotes (").</p> <p>To have the FortiGate unit search for a packet that does not contain the specified URI, add an exclamation mark (!) before the URI.</p> <p>Multiple content items can be specified in one rule. The value can contain mixed text and binary data. The binary data is generally enclosed within the pipe () character.</p> <p>The double quote ("), pipe sign () and colon (:) characters must be escaped using a back slash (\) if specified in a URI string.</p>
<code>--within <within_int>;</code>	<p>Use this together with the <code>distance</code> keyword to search for the contents within the specified number of bytes of the payload.</p> <p>The <code>within</code> value must be between 0 and 65535.</p>

Table 6: IP header keywords

Keyword and Value	Description
<code>--dst_addr [!]<ipv4>;</code>	<p>Use the <code>dst_addr</code> keyword to search for the destination IP address.</p> <p>To have the FortiGate search for a packet that does not contain the specified address, add an exclamation mark (!) before the IP address.</p> <p>You can define up to 28 IP addresses or CIDR blocks. Enclose the comma separated list in square brackets.</p> <p>Example: <code>dst_addr [172.20.0.0/16, 10.1.0.0/16, 192.168.0.0/16]</code></p>
<code>--ip_id <field_int>;</code>	Check the IP ID field for the specified value.
<code>--ip_option {rr eol nop ts sec lsrr ssrr satid any};</code>	<p>Use the <code>ip_option</code> keyword to check various IP option settings. The available options include:</p> <ul style="list-style-type: none"> <code>rr</code>: Check if IP RR (record route) option is present. <code>eol</code>: Check if IP EOL (end of list) option is present. <code>nop</code>: Check if IP NOP (no op) option is present. <code>ts</code>: Check if IP TS (time stamp) option is present. <code>sec</code>: Check if IP SEC (IP security) option is present. <code>lsrr</code>: Check if IP LSRR (loose source routing) option is present. <code>ssrr</code>: Check if IP SSRR (strict source routing) option is present. <code>satid</code>: Check if IP SATID (stream identifier) option is present. <code>any</code>: Check if IP any option is present.
<code>--ip_tos <field_int>;</code>	Check the IP TOS field for the specified value.
<code>--ip_ttl [< >] <ttl_int>;</code>	Check the IP time-to-live value against the specified value. Optionally, you can check for an IP time-to-live greater-than (>) or less-than (<) the specified value with the appropriate symbol.
<code>--protocol {<protocol_int> tcp udp icmp};</code>	<p>Check the IP protocol header.</p> <p>Example:</p> <pre>--protocol tcp;</pre>
<code>--src_addr [!]<ipv4>;</code>	<p>Use the <code>src_addr</code> keyword to search for the source IP address.</p> <p>To have the FortiGate unit search for a packet that does not contain the specified address, add an exclamation mark (!) before the IP address.</p> <p>You can define up to 28 IP addresses or CIDR blocks. Enclose the comma separated list in square brackets.</p> <p>Example: <code>src_addr 192.168.13.0/24</code></p>

Table 7: TCP header keywords

Keyword and Value	Description
<code>--ack <ack_int>;</code>	Check for the specified TCP acknowledge number.
<pre>--dst_port [!]{<port_int> :<port_int> <port_int>: <port_int>:<port_int>;</pre>	<p>Use the <code>dst_port</code> keyword to specify the destination port number.</p> <p>You can specify a single port or port range:</p> <ul style="list-style-type: none"> • <code><port_int></code> is a single port. • <code>:<port_int></code> includes the specified port and all lower numbered ports. • <code><port_int>:</code> includes the specified port and all higher numbered ports. • <code><port_int>:<port_int></code> includes the two specified ports and all ports in between.
<code>--seq <seq_int>;</code>	Check for the specified TCP sequence number.
<pre>--src_port [!]{<port_int> :<port_int> <port_int>: <port_int>:<port_int>;</pre>	<p>Use the <code>src_port</code> keyword to specify the source port number.</p> <p>You can specify a single port or port range:</p> <ul style="list-style-type: none"> • <code><port_int></code> is a single port. • <code>:<port_int></code> includes the specified port and all lower numbered ports. • <code><port_int>:</code> includes the specified port and all higher numbered ports. • <code><port_int>:<port_int></code> includes the two specified ports and all ports in between.

Table 7: TCP header keywords (Continued)

Keyword and Value	Description
<pre>--tcp_flags <SAFRUP120>[! * +] [, <SAFRUP120>];</pre>	<p>Specify the TCP flags to match in a packet.</p> <ul style="list-style-type: none"> • S: Match the SYN flag. • A: Match the ACK flag. • F: Match the FIN flag. • R: Match the RST flag. • U: Match the URG flag. • P: Match the PSH flag. • 1: Match Reserved bit 1. • 2: Match Reserved bit 2. • 0: Match No TCP flags set. • !: Match if the specified bits are not set. • *: Match if any of the specified bits are set. • +: Match on the specified bits, plus any others. <p>The first part if the value (<SAFRUP120>) defines the bits that must be present for a successful match. For example:</p> <pre>--tcp_flags AP</pre> <p>only matches the case where both A and P bits are set.</p> <p>The second part ([, <SAFRUP120>]) is optional, and defines the additional bits that can be present for a match. For example:</p> <pre>tcp_flags S,12</pre> <p>matches the following combinations of flags: S, S and 1, S and 2, S and 1 and 2.</p> <p>The modifiers !, * and + cannot be used in the second part.</p>
<pre>--window_size [!]<window_int>;</pre>	<p>Check for the specified TCP window size.</p> <p>You can specify the window size as a hexadecimal or decimal integer. A hexadecimal value must be preceded by 0x.</p> <p>To have the FortiGate search for the absence of the specified window size, add an exclamation mark (!) before the window size.</p>

Table 8: UDP header keywords

Keyword and Value	Description
<pre>--dst_port [!]{<port_int> :<port_int> <port_int>: <port_int>:<port_int>;</pre>	<p>Specify the destination port number.</p> <p>You can specify a single port or port range:</p> <ul style="list-style-type: none"> • <port_int> is a single port. • :<port_int> includes the specified port and all lower numbered ports. • <port_int>: includes the specified port and all higher numbered ports. • <port_int>:<port_int> includes the two specified ports and all ports in between.
<pre>--src_port [!]{<port_int> :<port_int> <port_int>: <port_int>:<port_int>;</pre>	<p>Specify the source port number.</p> <p>You can specify a single port or port range:</p> <ul style="list-style-type: none"> • <port_int> is a single port. • :<port_int> includes the specified port and all lower numbered ports. • <port_int>: includes the specified port and all higher numbered ports. • <port_int>:<port_int> includes the two specified ports and all ports in between.

Table 9: ICMP keywords

Keyword and Value	Usage
--icmp_code <code_int>;	Specify the ICMP code to match.
--icmp_id <id_int>;	Check for the specified ICMP ID value.
--icmp_seq <seq_int>;	Check for the specified ICMP sequence value.
--icmp_type <type_int>;	Specify the ICMP type to match.

Table 10: Other keywords

Keyword and Value	Description
<pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>;</pre>	<p>Test the packet payload size. With data_size specified, packet reassembly is turned off automatically. So a signature with data_size and only_stream values set is wrong.</p> <ul style="list-style-type: none"> • <size_int> is a particular packet size. • <<size_int> is a packet smaller than the specified size. • ><size_int> is a packet larger than the specified size. • <size_int><><size_int> is a packet within the range between the specified sizes.

Table 10: Other keywords (Continued)

Keyword and Value	Description
<code>--data_at <offset_int>[, relative];</code>	Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.
<code>--rate <matches_int>,<time_int>;</code>	<p>Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a specified number of times within a specified time period.</p> <ul style="list-style-type: none"> • <code><matches_int></code> is the number of times a signature must be detected. • <code><time_int></code> is the length of time in which the signature must be detected, in seconds. <p>For example, if a custom signature detects a pattern, a log entry will be created every time the signature is detected. If <code>--rate 100,10;</code> is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds.</p> <p>Use this command with <code>--track</code> to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all addresses.</p>
<code>--rpc_num <app_int>[, <ver_int> *][, <proc_int> *];</code>	Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wildcard can be used for version and procedure numbers.
<code>--same_ip;</code>	Check that the source and the destination have the same IP addresses.

Table 10: Other keywords (Continued)

Keyword and Value	Description
<code>--track {src_ip dst_ip dhcp_client };</code>	<p>When used with <code>--rate</code>, this keyword narrows the custom signature rate totals to individual addresses.</p> <ul style="list-style-type: none"> • <code>src_ip</code> has the FortiGate unit maintain a separate count of signature matches for each source address. • <code>dst_ip</code> has the FortiGate unit maintain a separate count of signature matches for each destination address. • <code>dhcp_client</code> has the FortiGate unit maintain a separate count of signature matches for each DHCP client. <p>For example, if <code>--rate 100,10</code> is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds. The FortiGate unit maintains a single total, regardless of source and destination address.</p> <p>If the same custom signature also includes <code>--track src_ip</code>; matches are totalled separately for each source address. A log entry is added when the signature is detected 100 times in 10 seconds within traffic from the same source address.</p> <p>Use of the <code>--track</code> keyword is invalid without the <code>--rate</code> keyword. The <code>--rate</code> keyword can be used without <code>--track</code>, however.</p>

IPS processing in an HA cluster

IPS processing in an HA cluster is no different than with a single FortiGate unit, from the point of view of the network user. The difference appears when a secondary unit takes over from the primary, and what happens depends on the HA mode.

Active-passive

In an active-passive HA cluster, the primary unit processes all traffic just as it would in a stand-alone configuration. Should the primary unit fail, a secondary unit will assume the role of the primary unit and begin to process network traffic. By default, the state of active communication sessions are not shared with secondary units and will not survive the fail-over condition. Once the sessions are reestablished however, traffic processing will continue as normal.

If your network requires that active sessions are taken over by the new primary unit, select *Enable Session Pick-up* in your HA configuration. Because session information must be sent to all subordinate units on a regular basis, session pick-up is a resource-intensive feature and is not enabled by default.

Active-active

The fail-over process in an active-active cluster is similar to an active-passive cluster. When the primary unit fails, a secondary unit takes over and traffic processing continues. The load-balancing schedule used to distribute sessions to the cluster members is used by the new primary unit to redistribute sessions among the remaining subordinate units. If session pick-up is not enabled, the sessions active on the failed primary are lost, and the sessions redistributed among the secondary units may also be lost. If session pick-up is enabled, all sessions are handled according to their last-known state.

For more information about HA options and settings, see the [FortiGate High Availability Handbook](#).

Configure IPS options

There are a number of CLI commands that influence how IPS functions.

Configuring the IPS engine algorithm

The IPS engine is able to search for signature matches in two ways. One method is faster but uses more memory, the other uses less memory but is slower. Use the `algorithm` CLI command to select one method:

```
config ips global
  set algorithm {high | low | engine-pick}
end
```

Specify `high` to use the faster more memory intensive method or `low` for the slower memory efficient method. The default setting is `engine-pick`, which allows the IPS engine to choose the best method on the fly.

Configuring the IPS engine-count

FortiGate units with multiple processors can run more than one IPS engine concurrently. The `engine-count` CLI command allows you to specify how many IPS engines are used at the same time:

```
config ips global
  set engine-count <int>
end
```

The recommended and default setting is 0, which allows the FortiGate unit to determine the optimum number of IPS engines.

Configuring fail-open

If the IPS engine fails for any reason, it will fail open by default. This means that traffic continues to flow without IPS scanning. If IPS protection is more important to your network than the uninterrupted flow of network traffic, you can disable this behavior using the `fail-open` CLI command:

```
config ips global
  set fail-open {enable | disable}
end
```

The default setting is `enable`.

Configuring the session count accuracy

The IPS engine can keep track of the number of open session in two ways. An accurate count uses more resources than a less accurate heuristic count.

```
config ips global
  set session-limit-mode {accurate | heuristic}
end
```

The default is heuristic.

Configuring the IPS buffer size

Set the size of the IPS buffer.

```
config ips global
  set socket-size <int>
end
```

The acceptable range is from 1 to 64 megabytes. The default size varies by model.

Configuring security processing modules

FortiGate Security Processing Modules, such as the CE4, XE2, and FE8, can increase overall system performance by accelerating some security and networking processing on the interfaces they provide. They also allow the FortiGate unit to offload the processing to the security module, thereby freeing up its own processor for other tasks. The security module performs its own IPS and firewall processing, but you can configure it to favor IPS in hostile high-traffic environments.

If you have a security processing module, use the following CLI commands to configure it to devote more resources to IPS than firewall. This example shows the CLI commands required to configure a security module in slot 1 for increased IPS performance.

```
config system amc-slot
  edit sw1
    set optimization-mode fw-ips
    set ips-weight balanced
    set ips-p2p disable
    set ips-fail-open enable
    set fp-disable none
    set ipsec-inb-optimization enable
    set syn-proxy-client-timer 3
    set syn-proxy-server-timer 3
  end
```

In addition to offloading IPS processing, security processing modules provide a hardware accelerated SYN proxy to defend against SYN flood denial of service attacks. When using a security module, configure your DoS sensor `tcp_syn_flood` anomaly with the *Proxy* action. The *Proxy* action activates the hardware accelerated SYN proxy.



Because DoS sensors are configured before being applied to an interface, you can assign a DoS sensor with the *Proxy* action to an interface that does not have hardware SYN proxy support. In this circumstance, the *Proxy* action is invalid and a *Pass* action will be applied.

Enable IPS packet logging

Packet logging saves the network packets containing the traffic matching an IPS signature to the attack log. The FortiGate unit will save the logged packets to wherever the logs are configured to be stored, whether memory, internal hard drive, a FortiAnalyzer unit, or the FortiGuard Analysis and Management Service.

You can enable packet logging in signature entries or in filters. Use caution in enabling packet logging in a filter. Filters configured with few restrictions can contain thousands of signatures, potentially resulting in a flood of saved packets. This would take up a great deal of space, require time to sort through, and consume considerable system resources to process. Packet logging is designed as a focused diagnostic tool and is best used with a narrow scope.



Although logging to multiple FortiAnalyzer units is supported, packet logs are not sent to the secondary and tertiary FortiAnalyzer units. Only the primary unit receives packet logs.

To enable packet logging for a signature

- 1 Create an IPS sensor. For more information, see [“Creating an IPS filter” on page 81](#).
- 2 Before saving the entry, select *Packet Log*.
- 3 Select the IPS sensor in the security policy that allows the network traffic the FortiGate unit will examine traffic for the signature.

To enable packet logging for a filter

- 1 Create a filter in an IPS sensor. For more information, see [“Creating an IPS filter” on page 81](#).
- 2 Before saving the filter, select *Enable All* for *Packet Logging*.
- 3 Select the IPS sensor in the security policy that allows the network traffic the FortiGate unit will examine for the signature.

For information on viewing and saving logged packets, see [“Viewing and saving logged packets” on page 280](#).

IPS examples

Configuring basic IPS protection

Small offices, whether they are small companies, home offices, or satellite offices, often have very simple needs. This example details how to enable IPS protection on a FortiGate unit located in a satellite office. The satellite office contains only Windows clients.

Creating an IPS sensor

Most IPS settings are configured in an IPS sensor. IPS sensors are selected in firewall policies. This way, you can create multiple IPS sensors, and tailor them to the traffic controlled by the security policy in which they are selected. In this example, you will create one IPS sensor.

To create an IPS sensor— web-based manager

- 1 Go to *UTM Profiles > Intrusion Protection > IPS Sensor*.
- 2 Select the *Create New* icon in the top of the Edit IPS Sensor window.
- 3 In the *Name* field, enter `basic_ips`.
- 4 In the *Comments* field, enter `IPS protection for Windows clients`.
- 5 Select *OK*.
- 6 Select the *Create New* drop-down and choose *Filter*.

- 7 For *Target*, select *Specify* and *Client*.
- 8 For *OS*, select *Specify* and *Windows*.
- 9 Select *OK* to save the filter.
- 10 Select *OK* to save the IPS sensor.

To create an IPS sensor — CLI

```
config ips sensor
edit basic_ips
set comment "IPS protection for Windows clients"
config filter
edit 1
set location client
set os windows
end
end
```

Selecting the IPS sensor in a security policy

An IPS sensor directs the FortiGate unit to scan network traffic only when it is selected in a security policy. When an IPS sensor is selected in a security policy, its settings are applied to all the traffic the security policy handles.

To select the IPS sensor in a security policy — web-based manager

- 1 Go to *Policy > Policy > Policy*.
- 2 Select a policy.
- 3 Select the *Edit* icon.
- 4 Enable *UTM*.
- 5 Select the *Enable IPS* option.
- 6 Select the `basic_ips` profile from the list.
- 7 Select *OK* to save the security policy.

To select the IPS sensor in a security policy — CLI

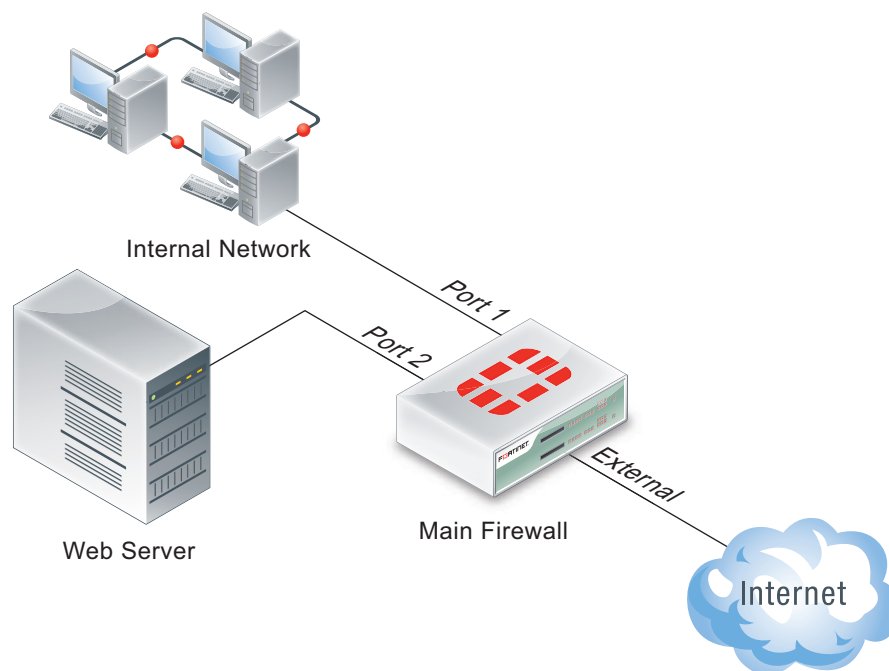
```
config firewall policy
edit 1
set utm-status enable
set ips-sensor basic_ips
end
```

All traffic handled by the security policy you modified will be scanned for attacks against Windows clients. A small office may have only one security policy configured. If you have multiple policies, consider enabling IPS scanning for all of them.

Using IPS to protect your web server

Many companies have web servers and they must be protected from attack. Since web servers must be accessible, protection is not as simple as blocking access. IPS is one tool your FortiGate unit has to allow you to protect your network.

In this example, we will configure IPS to protect a web server. As shown in [Figure 7 on page 105](#), a FortiGate unit protects a web server and an internal network. The internal network will have its own policies and configuration but we will concentrate on the web server in this example.

Figure 7: A simple network configuration

The FortiGate unit is configured with:

- a virtual IP to give the web server a unique address accessible from the Internet.
- a security policy to allow access to the web server from the Internet using the virtual IP.

To protect the web server using intrusion protection, you need to create an IPS sensor, populate it with filters, then enable IPS scanning in the security policy.

To create an IPS sensor

- 1 Go to *UTM Profiles > Intrusion Protection > IPS Sensor* and select *Create New*.
- 2 Enter `web_server` as the name of the new IPS sensor.
- 3 Select *OK*.

The new IPS sensor is created but it has no filters, and therefore no signatures are included.

The web server operating system is Linux, so you need to create a filter for all Linux server signatures.

To create the Linux server filter

- 1 Go to *UTM Profiles > Intrusion Protection > IPS Sensor* and select the `web_server` IPS sensor and select the *Edit* icon.
- 2 Select *Add Filter*.
- 3 Enter `Linux Server` as the name of the new filter.
- 4 For *Target*, select *Specify* and choose *server*.
- 5 For *OS*, select *Specify* and choose *Linux*.
- 6 Select *OK*.

The filter is saved and the IPS sensor page reappears. In the filter list, find the *Linux Server* filter and look at the value in the *Count* column. This shows how many signatures match the current filter settings. You can select the *View Rules* icon to see a listing of the included signatures.

The web server software is Apache, so you need to create a second filter for all Apache signatures.

To create the Apache filter

- 1 Go to *UTM Profiles > Intrusion Protection > IPS Sensor* and select the `web_server` IPS sensor and select the *Edit* icon.
- 2 Select *Add Filter*.
- 3 Enter `Apache` as the name of the new filter.
- 4 For *Application*, select *Specify* and choose *Apache* from the *Available* list.
- 5 Select the right-arrow to move *Apache* to the *Selected* list.
- 6 Select *OK*.

The filter is saved and the IPS sensor page reappears.

It might seem that you can skip a step and create one filter that specifies both Linux server and Apache signatures. However, this would include a smaller number of filters. It would not include signatures to detect attacks against the operating system directly, for example.

You have created the IPS sensor and the two filters that include the signatures you need. To have it start scanning traffic, you must edit the security policy.

To edit the security policy

- 1 Go to *Policy > Policy > Policy*, select security policy that allows access to the web server, and select the *Edit* icon.
- 2 Enable *UTM*.
- 3 Select the *Enable IPS* option and choose the `web_server` IPS sensor from the list.
- 4 Select *OK*.

Since IPS is enabled and the `web_server` IPS sensor is specified in the security policy controlling the web server traffic, the IPS sensor examines the web server traffic for matches to the signatures it contains.

Create and test a packet logging IPS sensor

In this example, you create a new IPS sensor and include a filter that detects the EICAR test file and saves a packet log when it is found. This is an ideal first experience with packet logging because the EICAR test file can cause no harm, and it is freely available for testing purposes.

Create an IPS sensor

- 1 Go to *UTM Profiles > Intrusion Protection > IPS Sensor*.
- 2 Select *Create New*.
- 3 Name the new IPS sensor `EICAR test`.
- 4 Select *OK*.

Create an entry

- 1 Select the *Create New* drop down menu and choose *Pre-defined Entry*.

- 2 Select the signature browse icon.
- 3 Rather than search through the signature list, use the name filter by selecting the filter icon in the header of the *Name* column.
- 4 In the *Filters* list, select *Name*.
- 5 Select *Enable*.
- 6 In the Field selection, choose *Contains*.
- 7 Enter `EICAR` in the Text field.
- 8 Select *OK*.
- 9 Select the *EICAR.AV.Test.File.Download* signature.
- 10 Select *OK*.
- 11 Select *Enable*, *Logging*, and *Packet Log*.
- 12 Select *OK*.
- 13 Select *Block* as the *Action*.
- 14 Select *OK* to save the IPS sensor.

You are returned to the IPS sensor list. The `EICAR test` sensor appears in the list.

Add the IPS sensor to the security policy allowing Internet access

- 1 Go to *Policy > Policy > Policy*.
- 2 Select the security policy that allows you to access the Internet.
- 3 Select the *Edit* icon.
- 4 Enable *Log Allowed Traffic*.
- 5 Enable *UTM*.
- 6 Select *Enable IPS*.
- 7 Choose `EICAR test` from the available IPS sensors.
- 8 Select *OK*.

With the IPS sensor configured and selected in the security policy, the FortiGate unit blocks any attempt to download the EICAR test file.

Test the IPS sensor

- 1 Using your web browser, go to http://www.eicar.org/anti_virus_test_file.htm.
- 2 Scroll to the bottom of the page and select *ecar.com* from the row labeled as using the standard HTTP protocol.
- 3 The browser attempts to download the requested file and,
 - If the file is successfully downloaded, the custom signature configuration failed at some point. Check the custom signature, the IPS sensor, and the firewall profile.
 - If the download is blocked with a high security alert message explaining that you're not permitted to download the file, the EICAR test file was blocked by the FortiGate unit antivirus scanner before the IPS sensor could examine it. Disable antivirus scanning and try to download the EICAR test file again.
 - If no file is downloaded and the browser eventually times out, the custom signature successfully detected the EICAR test file and blocked the download.

Viewing the packet log

- 1 Go to *Log&Report > Log & Archive Access > UTM Log*.

- 2 Locate the log entry that recorded the blocking of the EICAR test file block. The Message field data will be `tools: EICAR.AV.Test.File.Download`.
- 3 Select the *View Packet Log* icon in the *Packet Log* column.
- 4 The packet log viewer is displayed.

Creating a custom signature to block access to example.com

In this first example, you will create a custom signature to block access to the example.com URL.

This example describes the use of the custom signature syntax to block access to a URL. To create the custom signature entry in the FortiGate unit web-based manager, see [“Creating a custom IPS signature” on page 85](#).

- 1 Enter the custom signature basic format

All custom signatures have a header and at least one keyword/value pair. The header is always the same:

```
F-SBID( )
```

The keyword/value pairs appear within the parentheses and each pair is followed by a semicolon.

- 2 Choose a name for the custom signature

Every custom signature requires a name, so it is a good practice to assign a name before adding any other keywords.

Use the `--name` keyword to assign the custom signature a name. The name value follows the keyword after a space. Enclose the name value in double-quotes:

```
F-SBID( --name "Block.example.com"; )
```

The signature, as it appears here, will not do anything if you try to use it. It has a name, but does not look for any patterns in network traffic. You must specify a pattern that the FortiGate unit will search for.

- 3 Add a signature pattern

Use the `--pattern` keyword to specify what the FortiGate unit will search for:

```
F-SBID( --name "Block.example.com"; --pattern "example.com"; )
```

The signature will now detect the example.com URL appearing in network traffic. The custom signature should only detect the URL in HTTP traffic, however. Any other traffic with the URL should be allowed to pass. For example, an email message to or from example.com should not be stopped.

- 4 Specify the service

Use the `--service` keyword to limit the effect of the custom signature to only the HTTP protocol.

```
F-SBID( --name "Block.example.com"; --pattern "example.com";
--service HTTP; )
```

The FortiGate unit will limit its search for the pattern to the HTTP protocol. Even though the HTTP protocol uses only TCP traffic, the FortiGate will search for HTTP protocol communication in TCP, UDP, and ICMP traffic. This is a waste of system resources that you can avoid by limiting the search further, as shown below.

- 5 Specify the traffic type.

Use the `--protocol tcp` keyword to limit the effect of the custom signature to only TCP traffic. This will save system resources by not unnecessarily scanning UDP and ICMP traffic.

```
F-SBID( --name "Block.example.com"; --pattern "example.com";
--service HTTP; --protocol tcp; )
```

The FortiGate unit will limit its search for the pattern to TCP traffic and ignore UDP and ICMP network traffic.

6 Ignore case sensitivity

By default, patterns are case sensitive. If a user directed his or her browser to Example.com, the custom signature would not recognize the URL as a match.

Use the `--no_case` keyword to make the pattern matching case insensitive.

```
F-SBID( --name "Block.example.com"; --pattern "example.com";
--service HTTP; --no_case; )
```

Unlike all of the other keywords in this example, the `--no_case` keyword has no value. Only the keyword is required.

7 Limit pattern scans to only traffic sent from the client

The `--flow` command can be used to further limit the network traffic being scanned to only that sent by the client or by the server.

```
F-SBID( --name "Block.example.com"; --pattern "example.com";
--service HTTP; --no_case; --flow from_client; )
```

Web servers do not contact clients until clients first open a communication session. Therefore, using the `--flow from_client` command will force the FortiGate to ignore all traffic from the server. Since the majority of HTTP traffic flows from the server to the client, this will save considerable system resources and still maintain protection.

8 Specify the context

When the client browser tries to contact example.com, a DNS is first consulted to get the example.com server IP address. The IP address is then specified in the URL field of the HTTP communication. The domain name will still appear in the host field, so this custom signature will not function without the `--context host` keyword/value pair.

```
F-SBID( --name "Block.example.com"; --pattern "example.com";
--service HTTP; --no_case; --flow from_client;
--context host; )
```

Creating a custom signature to block the SMTP “vrfy” command

The SMTP “vrfy” command can be used to verify the existence of a single email address or to list all of the valid email accounts on an email server. A spammer could potentially use this command to obtain a list of all valid email users and direct spam to their inboxes.

In this example, you will create a custom signature to block the use of the vrfy command. Since the custom signature blocks the vrfy command from coming through the FortiGate unit, the administrator can still use the command on the internal network.

This example describes the use of the custom signature syntax to block the vrfy command. To create the custom signature entry in the FortiGate unit web-based manager, see [“Creating a custom IPS signature” on page 85](#).

1 Enter the custom signature basic format

All custom signatures have a header and at least one keyword/value pair. The header is always the same:

```
F-SBID( )
```

The keyword/value pairs appear within the parentheses and each pair is followed by a semicolon.

2 Choose a name for the custom signature

Every custom signature requires a name, so it is a good practice to assign a name before you add any other keywords.

Use the `--name` keyword to assign the custom signature a name. The name value follows the keyword after a space. Enclose the name value in double-quotes:

```
F-SBID( --name "Block.SMTP.VRFY.CMD"; )
```

The signature, as it appears here, will not do anything if you try to use it. It has a name, but does not look for any patterns in network traffic. You must specify a pattern that the FortiGate unit will search for.

3 Add a signature pattern

Use the `--pattern` keyword to specify what the FortiGate unit will search for:

```
F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy"; )
```

The signature will now detect the `vrfy` command appearing in network traffic. The custom signature should only detect the command in SMTP traffic, however. Any other traffic with the pattern should be allowed to pass. For example, an email message discussing the `vrfy` command should not be stopped.

4 Specify the service

Use the `--service` keyword to limit the effect of the custom signature to only the HTTP protocol.

```
F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy";  
--service SMTP; )
```

The FortiGate unit will limit its search for the pattern to the SMTP protocol.

Even though the SMTP protocol uses only TCP traffic, the FortiGate will search for SMTP protocol communication in TCP, UDP, and ICMP traffic. This is a waste of system resources that you can avoid by limiting the search further, as shown below.

5 Specify the traffic type.

Use the `--protocol tcp` keyword to limit the effect of the custom signature to only TCP traffic. This will save system resources by not unnecessarily scanning UDP and ICMP traffic.

```
F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy";  
--service SMTP; --protocol tcp; )
```

The FortiGate unit will limit its search for the pattern to TCP traffic and ignore the pattern in UDP and ICMP network traffic.

6 Ignore case sensitivity

By default, patterns are case sensitive. If a user directed his or her browser to `Example.com`, the custom signature would not recognize the URL as a match.

Use the `--no_case` keyword to make the pattern matching case insensitive.

```
F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy";  
--service SMTP; --no_case; )
```

Unlike all of the other keywords in this example, the `--no_case` keyword has no value. Only the keyword is required.

7 Specify the context

The SMTP `vrfy` command will appear in the SMTP header. The `--context host` keyword/value pair allows you to limit the pattern search to only the header.

```
F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy";  
--service SMTP; --no_case; --context header; )
```

Configuring a Fortinet Security Processing module

The Example Corporation has a web site that is the target of SYN floods. While they investigate the source of the attacks, it's very important that the web site remain accessible. To enhance the ability of the company's FortiGate-620B to deal with SYN floods, the administrator will install an ASM-CE4 Fortinet Security Processing module and have all external access to the web server come through it.

The security processing modules not only accelerate and offload network traffic from the FortiGate unit's processor, but they also accelerate and offload security and content scanning. The ability of the security module to accelerate IPS scanning and DoS protection greatly enhances the defense capabilities of the FortiGate-620B.

Assumptions

As shown in other examples and network diagrams throughout this document, the Example Corporation has a pair of FortiGate-620B units in an HA cluster. To simplify this example, the cluster is replaced with a single FortiGate-620B.

An ASM-CE4 is installed in the FortiGate-620B.

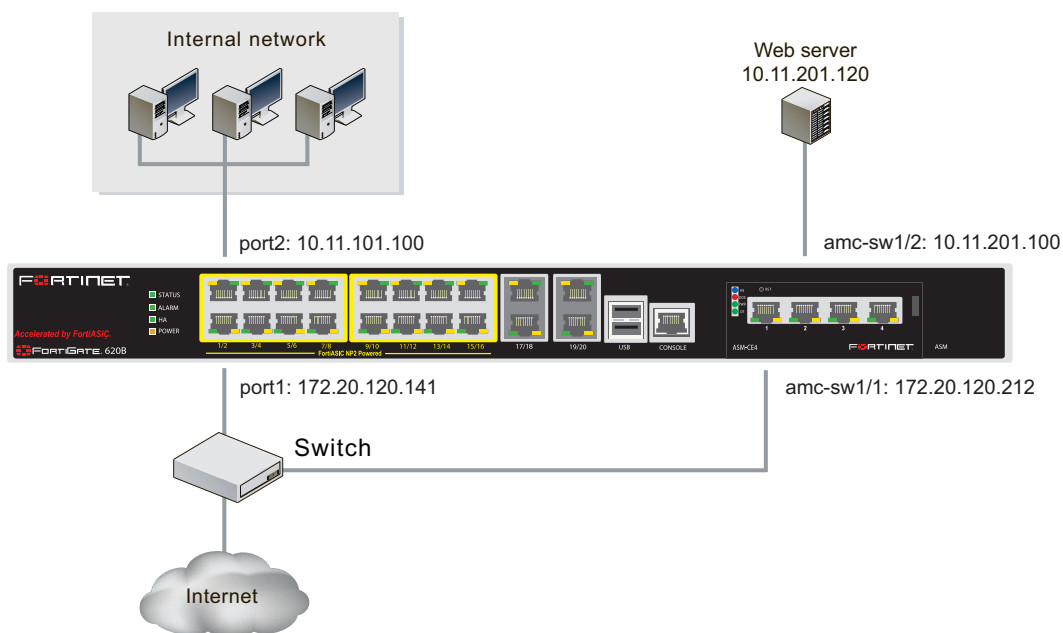
The network is configured as shown in [Figure 8](#).

Network configuration

The Example Corporation network needs minimal changes to incorporate the ASM-CE4. Interface amc-sw1/1 of the ASM-CE4 is connected to the Internet and interface amc-sw1/1 is connected to the web server.

Since the main office network is connected to port2 and the Internet is connected to port1, a switch is installed to allow both port1 and amc-sw1/1 to be connected to the Internet.

Figure 8: The FortiGate-620B network configuration



The switch used to connect port1 and amc-sw1/1 to the Internet must be able to handle any SYN flood, all of the legitimate traffic to the web site, and all of the traffic to and from the Example Corporation internal network. If the switch can not handle the bandwidth, or if the connection to the service provider can not provide the required bandwidth, traffic will be lost.

Security module configuration

The Fortinet security modules come configured to give equal priority to content inspection and firewall processing. The Example Corporation is using a ASM-CE4 module to defend its web server against SYN flood attacks so firewall processing is a secondary consideration.

Use these CLI commands to configure the security module in ASM slot 1 to devote more resources to content processing, including DoS and IPS, than to firewall processing.

```
config system amc-slot
edit sw1
    set optimization-mode fw-ips
    set ips-weight balanced
    set ips-p2p disable
    set ips-fail-open enable
    set fp-disable none
    set ipsec-inb-optimization enable
    set syn-proxy-client-timer 3
    set syn-proxy-server-timer 3
end
```

These settings do not disable firewall processing. Rather, when the security module nears its processing capacity, it will chose to service content inspection over firewall processing.

DoS sensor configuration

Defend against anomaly-based attacks using a DoS sensor. For the SYN floods launched against the Example Corporation web site, the *tcp_syn_flood* anomaly is the best defense.

Create a DoS sensor for SYN flood protection

- 1 Go to *UTM Profiles > Intrusion Protection > DoS Sensor*.
- 2 Select *Create New*.
- 3 Enter *Web site SYN protection* for the DoS sensor name.
- 4 Select *OK* to create the sensor.

The default *tcp_syn_flood* threshold is 2000. This means that the configured action will be triggered when the number of TCP packets with the SYN flag set exceeds 2000 per second.

For some applications, this value will be too high, while for others it will be too low. One way to find the correct values for your environment is to set the action to *Pass* and enable logging. Observe the logs and adjust the threshold values until you can determine the value at which normal traffic begins to generate attack reports. Set the threshold above this value with the margin you want. Note that the smaller the margin, the more protected your network will be from DoS attacks, but your network traffic will also be more likely to generate false alarms.

Configure a DoS sensor for SYN flood protection

- 1 Go to *UTM Profiles > Intrusion Protection > DoS Sensor*.
- 2 Select the `Web site SYN protection` sensor and select the *Edit* icon.
- 3 Select *Enable* and *Logging* for the `tcp_syn_flood` anomaly.
- 4 Select the *Proxy* action for the `tcp_syn_flood` anomaly.
- 5 Enter the threshold value for the `tcp_syn_flood` anomaly.
- 6 Select *OK*.

With the action configured as *Proxy*, TCP packets with the SYN flag set will be passed until the threshold value is exceeded. At that point, TCP packets with the SYN flag set until their numbers fall below the threshold value.

The ASM-CE4 security module will intercept the packet, and reply to the client with a TCP packet that has the SYN and ACK flags set. If the connection request is legitimate, the client will reply with a packet that has the ACK flag set. The ASM-CE4 will then 'replay' this exchange to the server and allow the client and server to communicate directly.

If the client does not reply with the expected packet, the ASM-CE4 will close the connection. Therefore, if the security module receives a flood of SYN packets, they will be blocked. Only the legitimate connections will be allowed through to the server.

DoS policy configuration

Before the DoS sensor can begin examining network traffic, you must create and configure a DoS policy and specify the DoS sensor.

Create a DoS policy

- 1 Go to *Policy > Policy > DoS Policy*.
- 2 Select *Create New*.
- 3 Select `amc-sw1/1` for *Source Interface/Zone*.
- 4 Select *all* for *Source Address*.
- 5 Select *all* for *Destination Address*.
- 6 Select *ANY* for *Service*.
- 7 Enable *DoS Sensor* and select the `Web site SYN protection` sensor from the list.
- 8 Select *OK*.

Virtual IP configuration

Traffic destined for the web server will arrive at the `amc-sw1/1` interface. You must create a virtual IP mapping to have the ASM-CE4 direct the traffic to the web server.

Create a virtual IP mapping

- 1 Go to *Firewall Objects > Virtual IP > Virtual IP*.
- 2 Select *Create New*.
- 3 In the *Name* field, enter `web_server`.
- 4 Select `amc-sw1/1` as the *External Interface*.
- 5 Enter `172.20.120.212` as the *External IP Address/Range*.
- 6 Enter `10.11.201.120` as the *Mapped IP Address/Range*.
- 7 Select *OK*.

Security policy configuration

A security policy is required to allow traffic through to the web server. Further, the security policy must include the virtual IP so the traffic is directed to the web server.

Create a security policy

- 1 Go to *Policy > Policy > Policy*.
- 2 Select *Create New*.
- 3 Select *amc-sw1/1* for the *Source Interface/Zone*.
- 4 Select *all* for the *Source Address*.
- 5 Select *amc-sw1/2* for the *Destination Interface/Zone*.
- 6 Select *web_server* for the *Destination Address*.
- 7 Select *Enable NAT*.
- 8 Select *OK*.

Attempts to connect to 172.20.120.212 will be forwarded to the web server with this security policy in place.

View proxy statistics

With a FortiGate security module installed, a CLI command displays the current proxy statistics.

At the CLI prompt, type `execute npu-cli /dev/ce4_0 showsynproxy`. The last nine lines will list the proxy statistics:

```

Total Proxied TCP Connections:      434055223
Working Proxied TCP Connections:    515699
Retired TCP Connections:            433539524
Valid TCP Connections:              0
Attacks, No Ack From Client:        433539524
No SynAck From Server:              0
Rst By Server (service not supported): 0
Client timeout setting:             3 Seconds
Server timeout setting:             3 Seconds

```

Total Proxied TCP Connections	The number of proxied TCP connection attempts since the FortiGate unit was restarted. This value is the sum of the working and retired connection totals.
Working Proxied TCP Connections	The number of TCP connection attempts currently being proxied.
Retired TCP Connections	The number of proxied TCP connection attempts dropped or allowed. These connection attempts are no-longer being serviced. This value is the sum of the valid and attacks totals.
Valid TCP Connections	The number of valid proxied TCP connection attempts.
Attacks, No Ack From Client	The number of proxied TCP connection attempts in which the client did not reply. These are typically attacks.

No SynAck From Server	The number of valid client connection attempts in which the server does not reply.
Rst By Server (service not supported)	The number of valid client connection attempts in which the server resets the connection.
Client timeout setting	The client time-out duration.
Server timeout setting	The server time-out duration.

Intrusion Protection interface reference

The Intrusion Protection system combines signature and anomaly detection and prevention with low latency and excellent reliability. With Intrusion Protection, you can create multiple IPS sensors, each containing a complete configuration based on signatures. Then, you can apply any IPS sensor to a firewall policy. You can also create DoS sensors to examine traffic for anomaly-based attacks.

This topic contains the following:

- [IPS Sensor](#)
- [DoS sensor](#)
- [Predefined](#)
- [Custom](#)
- [Protocol Decoder](#)

IPS Sensor

You can group signatures into IPS sensors for easy selection when applying to firewall policies. You can define signatures for specific types of traffic in separate IPS sensors, and then select those sensors in profiles designed to handle that type of traffic. For example, you can specify all of the web-server related signatures in an IPS sensor, and that sensor can then be applied to a firewall policy that controls all of the traffic to and from a web server protected by the unit.

The FortiGuard Service periodically updates the pre-defined signatures, with signatures added to counter new threats. Since the signatures included in filters are defined by specifying signature attributes, new signatures matching existing filter specifications will automatically be included in those filters. For example, if you have a filter that includes all signatures for the Windows operating system, your filter will automatically incorporate new Windows signatures as they are added.

Each IPS sensor consists of two parts: filters and overrides. Overrides are always checked before filters.

Each filter consists of a number of signatures attributes. All of the signatures with those attributes, and only those attributes, are checked against traffic when the filter is run. If multiple filters are defined in an IPS Sensor, they are checked against the traffic one at a time, from top to bottom. If a match is found, the unit takes the appropriate action and stops further checking.

A signature override can modify the behavior of a signature specified in a filter. A signature override can also add a signature not specified in the sensor's filters. Custom signatures are included in an IPS sensor using overrides.

The signatures in the overrides are first compared to network traffic. If the IPS sensor does not find any matches, it then compares the signatures in each filter to network traffic, one filter at a time, from top to bottom. If no signature matches are found, the IPS sensor allows the network traffic.

The signatures included in the filter are only those matching every attribute specified. When created, a new filter has every attribute set to *all* which causes every signature to be included in the filter. If the severity is changed to high, and the target is changed to server, the filter includes only signatures checking for high priority attacks targeted at servers.

IPS sensor configuration settings

The following are IPS sensor configuration settings in *UTM Profiles > Intrusion Protection > IPS Sensor*.

IPS Sensor page Lists each individual IPS sensor, either default or ones that you created. On this page you can edit, delete or create a new IPS sensor. If you want to configure tags, and the tag options are not available on the web-based manager, you must enable tag options by going to <i>System > Admin > Settings</i> . Note: You can configure IPS signatures to not be triggered until the threshold is met; however, this is configured only in the CLI. You must use <code>config override in config ips sensor</code> command to configure this option.	
Create New	Creates a new IPS sensor. When you select <i>Create New</i> , you are automatically redirected to the New IPS Sensor page. This page provides a name field and comment field. You must enter a name to go the IPS Sensor Settings page.
Delete	Removes the IPS sensor from the list. To remove multiple IPS sensors from within the list, on the IPS Sensor page, in each of the rows of the sensors you want removed, select the check box and then select <i>Delete</i> . To remove all IPS sensors from the list, on the IPS Sensor page, select the check box in the check box column and then select <i>Delete</i> .
Edit	Modifies settings within an IPS sensor. When you select <i>Edit</i> , you are automatically redirected to the Edit IPS Sensor page.
Name	The name of each IPS sensor.
Comments	An optional description of the IPS sensor.

Ref.	<p>Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a firewall policy; on the Profile page (<i>UTM Profiles > Antivirus > Profile</i>), 1 appears in <i>Ref.</i>.</p> <p>To view the location of the referenced object, select the number in <i>Ref.</i>, and the Object Usage window appears displaying the various locations of the referenced object.</p> <p>To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:</p> <ul style="list-style-type: none"> • View the list page for these objects – automatically redirects you to the list page where the object is referenced at. • Edit this object – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • View the details for this object – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy, and that firewall policy's settings appear within the table.
all_default (default)	Includes all signatures. The sensor is set to use the default enable status and action of each signature.
all_default_pass (default)	Includes all signatures. The sensor is set to use the default enable status of each signature, but the action is set to pass.
protect_client (default)	Includes only the signatures designed to detect attacks against clients and uses the default enable status and action of each signature.
protect_email_server (default)	Includes only the signatures designed to detect attacks against servers and the SMTP, POP3, or IMAP protocols and uses the default enable status and action of each signature.
protect_http_server (default)	Includes only the signatures designed to detect attacks against servers and the HTTP protocol and uses the default enable status and action of each signature.
<p>Edit IPS Sensor page</p> <p>Provides settings for configuring multiple filters and overrides that make up an IPS sensor. The Edit IPS Sensor Settings page contains two sections, one called Filters where you can configure filters and the other called Overrides where you can configure either predefined or custom overrides.</p> <p>Note: Logging is enabled in the CLI.</p>	
Name	If you are editing an existing IPS sensor and you want to change the name, enter a new name in the field. You must select <i>Apply</i> to save the change.

Comments	If you are editing an existing IPS sensor and you want to change the description, enter the changes in the field. You must select <i>Apply</i> to save the change.
Create New	Creates a new filter. You can also use the Insert icon to create a new filter for an IPS sensor. When you select <i>Create New</i> , you are automatically redirected to the Edit IPS Filter page. If you want to create a predefined override or a custom override, select the down arrow beside <i>Create New</i> . From the list, you can select <i>Pre-defined Entry</i> , which creates a predefined override, or you can select <i>Custom Entry</i> , which creates a custom override. For more information about overrides, see “Pre-defined overrides and custom overrides configuration settings” on page 120 .
Edit	Modifies settings within a filter. When you select <i>Edit</i> , you are automatically redirected to the Edit IPS Filter page.
Delete	Removes a filter from the list within the Filters section of the IPS Sensor Settings page. To remove multiple filter lists from within the list, in the Filters section, in each of the rows of the filters you want removed, select the check box and then select <i>Delete</i> . To remove all filters from the list, in the Filters section, select the check box in the check box column and then select <i>Delete</i> .
Insert	Inserts a new filter in filter list in the list in the Filters section. When you select <i>Insert</i> , you are automatically redirected to the Edit IPS Filter page.
Move To	Moves a filter to any position within the list in the Filters section. You must select the check box in the row of the filter you want moved so that filter will be moved within the list. When you select <i>Move To</i> , the following appears: <code>Please enter the destination filter position.</code> Enter the number for the filter's new position within the list, for example, 5, to place the first entry in the fifth position Select <i>OK</i> .
View Rules	View the rules of a filter. When you select <i>View Rules</i> , the Matched Rules window appears. Scroll through the list to see all the rules within that filter.
ID	The identification number of the entry you created.
Severity	The severity level of the filter.
Target	The target specified for that filter.
Protocol	The type of protocol for that filter.
OS	The type of operating system.
Application	The software application, such as Adobe.

Enable	A green check mark appears if you select <i>Enable all</i> within the filter's settings. If you select <i>Disable all</i> , a gray x appears. Note: For the default IPS sensor (called "default") the word <i>Default</i> displays instead of the check mark. It cannot be disabled.
Action	The type of action the unit will take. This action can be <i>Block</i> , <i>Pass</i> , or <i>Reset</i> .
Packet Logging	A green checkmark appears if you select <i>Enable all</i> within the filter's settings. A gray x appears if you select <i>Disable all</i> .
Matched Signatures	The number of signatures included in the filter. Overrides are not included in the total.

Filters configuration settings

A filter is a collection of signature attributes that you specify. The signatures that have all of the attributes specified in a filter are included in the IPS signature. An IPS sensor can contain multiple IPS filters. The following are the available options when configuring filters.

The following are filter configuration settings for an IPS sensor in *UTM Profiles > Intrusion Protection > IPS Sensors*.

New IPS Filter page Provides settings for configuring a filter. You are automatically redirected to this page when you select <i>Create New</i> in the <i>Filters</i> section of the IPS Sensor Settings page.	
Name	Enter a name for the filter.
Severity	Select a severity level. You must specify a severity level if you do not want to all severity levels.
Target	Select the type of system targeted by the attack.
OS	Select to specify the type of operating system, or select All to include all operating systems. The operating system available include BSD and Solaris. Signatures with an OS attack attribute of All affect all operating system and these signatures are automatically included in any filter regardless of whether a single, multiple, or all operating systems are specified.
Protocol	Select to choose multiple protocols or all available protocols. To select specific protocols, select <i>Specify</i> , and then move each protocol that you want from the Available column to the Selected column using the -> arrow. To remove a protocol from the Selected column, select the protocol and then use the <- arrow to move the protocol back to the Available column.
Application	Select to choose multiple applications or all available applications. To select specific applications, select <i>Specify</i> , and then move each application that you want from the Available list to the Selected list using the -> arrow. To remove an application from the Selected list, select the protocol and then use the <- arrow to move the application back to the Available list.

Tags	Applies tags to the file filter only. These tags do not display within the Filters section, only within the filter itself on the Edit IPS Filter page. If you do not see <i>Tags</i> and its available settings, go to <i>System > Admin > Settings</i> to enable them on the web-based manager.
Applied tags	Displays the tags that you have added to the filter.
Add tags	Enter the tag in the field and then select the plus (+) sign to add the tag to the filter. This also adds the tag to the <i>Applied tags</i> list.
Enable All Matching Signatures	Select to accept the defaults, or enable all signatures, or disable all.
Action When Signature Is Triggered	Select to indicate to the unit what action to take when a signature is triggered. When you select <i>Accept signature defaults</i> , and then select to enable <i>Quarantine Attackers (to Banned Users List)</i> , the <i>Method</i> and <i>Expires</i> options display. The <i>Quarantine Attackers (to Banned Users List)</i> appears only when <i>Accept signature defaults</i> is selected.
Quarantine Attackers (to Banned Users List)	Select if you want to add an attacker to the <i>Banned Users List</i> .
Method	Select <i>Attacker's IP Address</i> to block all traffic sent from the attacker's IP address. Traffic from the attacker's IP address is blocked because the attacker's IP address is in the Banned Users List. Select <i>Attacker and Victim IP Addresses</i> to block all traffic sent from the attacker IP address to the target (victim) IP address. Traffic from the attacker IP address to addresses other than the victim IP address is allowed. The attacker and target IP addresses are added to the banned user list as one entry. Select <i>Attack's Incoming Interface</i> to block all traffic from connecting to the Fortinet interface that received the attack. The interface is added to the banned user list.
Expires	You can select whether the attacker is banned indefinitely or for a specified number of days, hours, or minutes. Select <i>Indefinitely</i> if you do not want the information to expire. Select <i>After</i> and enter the number of hours, minutes or days.
Packet Logging	Select to enable packet logging on the filter. When you select to enable packet logging on a filter, the unit saves a copy of the packets that triggered an attack detection for future analysis or for audit purposes. Note: You must enable logging for both filter and sensor so that logging occurs. The logging option is available only in the CLI.

Pre-defined overrides and custom overrides configuration settings

Pre-defined and custom overrides are configured and work mainly in the same way as filters. Unlike filters, each override defines the behavior of one signature.

Overrides can be used in two ways:

- Change the behavior of a signature already included in a filter. For example, to protect a web server, you could create a filter that includes and enables all signatures related to servers. If you wanted to disable one of those signatures, the simplest way would be to create an override and mark the signature as disabled.
- Add an individual signature that is not included in any filters to an IPS sensor. This is the only way to add custom signatures to IPS sensors.

When a pre-defined signature is specified in an override, the default status and action attributes have no effect. These settings must be explicitly set when creating the override.

When configuring either a pre-defined override or a custom override, the following options are available regardless which override you are configuring.

Predefined and custom overrides are configured in the IPS Sensor itself, located in *UTM Profiles > Intrusion Protection > IPS Sensors*. The following are configuration settings for both predefined and custom overrides.



Before an override can affect network traffic, you must add it to a filter, and you must select the IPS sensor and then apply it to a policy. An override does not have the ability to affect network traffic until these steps are taken.

Configure IPS Entry page

Provides settings for configuring both predefined overrides and custom overrides. You are automatically redirected to this page after selecting either *Pre-defined Entry* or *Custom Entry*, which is accessed when you select the down arrow beside *Create New*.

Note: Logging is enabled in the CLI.

Signature	Select the browse icon to view the list of available signatures. From this list, select a signature the override will apply to and then select <i>OK</i> .
Enable	Select to enable the signature override.
Action	Select <i>Pass</i> , <i>Block</i> or <i>Reset</i> . When the override is enabled, the action determines what the unit will do with traffic containing the specified signature.
Packet Log	Select to save packets that trigger the override to the unit's hard drive for later examination.
Quarantine Attackers (to Banned Users List)	Select to enable NAC quarantine for this override. The unit deals with the attack according to the IPS sensor or DoS sensor configuration regardless of this setting.

Method	<p>Select <i>Attacker's IP address</i> to block all traffic sent from the attackers IP address. The attackers IP address is also added to the banned user list. The target address is not affected.</p> <p>Select <i>Attacker and Victim IP Addresses</i> to block all traffic sent from the attacker IP address to the target (victim) IP address. Traffic from the attacker IP address to addresses other than the victim IP address is allowed. The attacker and target IP addresses are added to the banned user list as one entry.</p> <p>Select <i>Attack's Incoming Interface</i> to block all traffic from connecting to the Fortinet interface that received the attack. The interface is added to the banned user list.</p>
Expires	You can select whether the attacker is banned indefinitely or for a specified number of days, hours, or minutes.
Exempt IP	Enter IP addresses to exclude from the override. The override will then apply to all IP addresses except those defined as exempt. The exempt IP addresses are defined in pairs, with a source and destination, and traffic moving from the source to the destination is exempt from the override.
Source	The exempt source IP address. Enter 0.0.0.0/0 to include all source IP addresses.
Destination:	The exempt destination IP address. Enter 0.0.0.0/0 to include all destination IP addresses.
Add	Select to add other exempt IP addresses to the list in the table below Add.
#	The number identifying the order of the item in the list.
Source	The source IP address and netmask entered.
Destination	The destination IP address and netmask entered.
Delete	Select to remove an item in the list.

DoS sensor

IPS uses a traffic anomaly detection feature to identify network traffic that does not fit known or common traffic patterns and behavior. For example, one type of flooding is the denial of service (DoS) attack that occurs when an attacking system starts an abnormally large number of sessions with a target system. The large number of sessions slows down or disables the target system so legitimate users can no longer use it. This type of attack gives the DoS sensor its name, although it is capable of detecting and protecting against a number of anomaly attacks.

You can enable or disable logging for each traffic anomaly, and configure the detection threshold and action to take when the detection threshold is exceeded.

You can create multiple DoS sensors. Each sensor consists of 12 anomaly types that you can configure. When a sensor detects an anomaly, it applies the configured action. One sensor can be selected for use in each DoS policy, allowing you to configure the anomaly thresholds separately for each interface. Multiple sensors allow great granularity in detecting anomalies because each sensor can be configured for the specific needs of the interface it is attached to by the DoS policy.

The traffic anomaly detection list can be updated only when the firmware image is upgraded on the unit.

Since an improperly configured DoS sensor can interfere with network traffic, no DoS sensors are present on a factory default unit. You must create your own and then select them in a DoS policy before they will take effect. Thresholds for newly created sensors are preset with recommended values that you can adjust to meet the needs of your network.



It is important to know normal and expected network traffic before changing the default anomaly thresholds. Setting the thresholds too low could cause false positives, and setting the thresholds too high could allow otherwise avoidable attacks.



If virtual domains are enabled on the unit, the Intrusion Protection settings must be configured separately in each VDOM. All sensors and custom signatures will appear only in the VDOM in which they were created.

DoS sensor configuration settings

The following are DoS sensor configuration settings in *UTM Profiles > Intrusion Protection > DoS Sensor*.

DoS Sensor page

Lists each default DoS sensor and each DoS sensor that you created. On this page, you can create, edit or delete a DoS sensor.

Create New	Creates a new DoS sensor. When you select <i>Create New</i> , you are automatically redirected to the New DoS Sensor page. The New DoS Sensor page provides a name field and a comment file. You must enter a name to go to the Edit DoS Sensor page.
Edit	Modifies the settings within a DoS sensor. You can modify the following information: Action, Severity, and Threshold. When you select <i>Edit</i> , you are automatically redirected to the Edit DoS Sensor page.
Delete	Removes a DoS sensor from the list on the DoS Sensor page. To remove multiple DoS sensors from within the list, on the DoS Sensor page, in each of the rows of the sensors you want removed, select the check box and then select <i>Delete</i> . To remove all DoS sensors from the list, on the DoS Sensor page, select the check box in the check box column and then select <i>Delete</i> .
Name	The DoS sensor name.
Comments	An optional description of the DoS sensor.

Ref.	<p>Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a firewall policy; on the Profile page (<i>UTM Profiles > Antivirus > Profile</i>), 1 appears in <i>Ref.</i>.</p> <p>To view the location of the referenced object, select the number in <i>Ref.</i>, and the Object Usage window appears displaying the various locations of the referenced object.</p> <p>To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:</p> <ul style="list-style-type: none"> • View the list page for these objects – automatically redirects you to the list page where the object is referenced at. • Edit this object – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • View the details for this object – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy, and that firewall policy's settings appear within the table.
Edit DoS Sensor page Provides settings for configuring the action type, threshold amount, and if logging should be enabled for the anomaly. There are twelve default anomalies to configure settings for. If you are editing a DoS Sensor, you are redirected to this page.	
Name	If you are editing an existing DoS sensor setting and want to change the name, enter a new name in this field. You must select <i>OK</i> to save the change.
Comments	If you are editing an existing DoS sensor setting and want to change or add a description, enter the new text in this field. You must select <i>OK</i> to save these changes.
Anomalies Configuration	
Name	The name of the anomaly.
Enable	Select the check box to enable the DoS sensor to detect when the specified anomaly occurs. Selecting the check box in the header row will enable all anomalies.
Logging	Select the check box to enable the DoS sensor to log when the anomaly occurs. Selecting the check box in the header row will enable logging for all anomalies. Anomalies that are not enabled are not logged.

Action	Select <i>Pass</i> to allow anomalous traffic to pass when the unit detects it, or set <i>Block</i> to prevent the traffic from passing.
Threshold	Displays the number of sessions/packets that must show the anomalous behavior before the Fortinet unit triggers the anomaly action (pass or block). If required, change the number. Range 1 to 2 147 483 647. For more information about how these settings affect specific anomalies, see Table 12 on page 125 and “ SYN threshold (preventing SYN floods using a DoS sensor) ” on page 125.

SYN proxy

Fortinet units with Fortinet security processing modules installed offer a third action for the tcp_syn_flood threshold when a module is installed. Instead of Block and Pass, you can choose to Proxy the incomplete connections that exceed the threshold value.

When the tcp_syn_flood threshold action is set to proxy, incomplete TCP connections are allowed as normal as long as the configured threshold is not exceeded. If the threshold is exceeded, the unit will intercept incoming SYN packets from clients and respond with a SYN+ACK packet. If the unit receives an ACK response as expected, it will “replay” this exchange to the server to establish a communication session between the client and the server, and allow the communication to proceed.

SYN threshold (preventing SYN floods using a DoS sensor)

The preferred primary defense against any type of SYN flood is the DoS sensor tcp_syn_flood threshold. The threshold value sets an upper limit on the number of new incomplete TCP connections allowed per second. If the number of incomplete connections exceeds the threshold value, and the action is set to Pass, the unit will allow the SYN packets that exceed the threshold. If the action is set to Block, the unit will block the SYN packets that exceed the threshold, but it will allow SYN packets from clients that send another SYN packet.

The tools attackers use to generate network traffic will not send a second SYN packet with a SYN+ACK response is not received from the server. These tools will not “retry”. Legitimate clients will retry when no response is received, and these retries are allowed even if they exceed the threshold with the action set to Block.

Understanding the anomalies

Each DoS sensor offers four configurable statistical anomaly types for each of the TCP, UDP, and ICMP protocols.

Table 11: The four statistical anomaly types.

For each of the TCP, UDP, and ICMP protocols, DoS sensors offer four statistical anomaly types. The result is twelve configurable anomalies, which are shown in [Table 12](#).

Table 12: The twelve individually configurable anomalies

Anomaly	Description
tcp_syn_flood	If the SYN packet rate, including retransmission, to one destination IP address exceeds the configured threshold value, the action is executed. The threshold is expressed in packets per second.

Table 12: The twelve individually configurable anomalies (Continued)

Anomaly	Description
<code>tcp_port_scan</code>	If the SYN packets rate, including retransmission, from one source IP address exceeds the configured threshold value, the action is executed. The threshold is expressed in packets per second.
<code>tcp_src_session</code>	If the number of concurrent TCP connections from one source IP address exceeds the configured threshold value, the action is executed.
<code>tcp_dst_session</code>	If the number of concurrent TCP connections to one destination IP address exceeds the configured threshold value, the action is executed.
<code>udp_flood</code>	If the UDP traffic to one destination IP address exceeds the configured threshold value, the action is executed. The threshold is expressed in packets per second.
<code>udp_scan</code>	If the number of UDP sessions originating from one source IP address exceeds the configured threshold value, the action is executed. The threshold is expressed in packets per second.
<code>udp_src_session</code>	If the number of concurrent UDP connections from one source IP address exceeds the configured threshold value, the action is executed.
<code>udp_dst_session</code>	If the number of concurrent UDP connections to one destination IP address exceeds the configured threshold value, the action is executed.
<code>icmp_flood</code>	If the number of ICMP packets sent to one destination IP address exceeds the configured threshold value, the action is executed. The threshold is expressed in packets per second.
<code>icmp_sweep</code>	If the number of ICMP packets originating from one source IP address exceeds the configured threshold value, the action is executed. The threshold is expressed in packets per second.
<code>icmp_src_session</code>	If the number of concurrent ICMP connections from one source IP address exceeds the configured threshold value, the action is executed.
<code>icmp_dst_session</code>	If the number of concurrent ICMP connections to one destination IP address exceeds the configured threshold value, the action is executed.

Predefined

The Intrusion Protection system can use signatures once you have grouped the required signatures in an IPS sensor. If required, you can override the default settings of the signatures specified in an IPS sensor. The unit provides a number of pre-built IPS sensors, but you should check their settings before using them, to ensure they meet your network requirements.

By using only the signatures you require, you can improve system performance and reduce the number of log messages and alert email messages that the IPS sensor generates. For example, if the unit is not protecting a web server, web server signatures are not included.

The predefined signature list, located in *UTM Profiles > Intrusion Protection > Predefined*, includes signatures that are currently in the [FortiGuard Center Vulnerability Encyclopedia](#). This encyclopedia also includes additional signatures not found in the Predefined menu. Each signature name is a link to the vulnerability encyclopedia entry for the signature. The vulnerability encyclopedia describes the attack detected by the signature and provides recommended actions and links for more information.

The predefined signature list also includes characteristics such as the severity level of the attack, protocol, and applications affected for each signature. These characteristics give you a quick reference to what the signature is for. You can also use these characteristics to sort the signature list, grouping signatures by common characteristics. The signature list also displays the default action, the default logging status, and whether the signature is enabled by default. The signatures are sorted by name, which is default. The predefined signature list table allows you to view these characteristics in detail. The table is located at the bottom of the page; however, you can customize the table so that it appears on the right side of the page or hidden.

Viewing predefined signatures

You can view predefined signatures in *UTM Profiles > Intrusion Protection > Predefined*.

When you are viewing signatures, you can view each one in detail, from the IPS signatures viewer table. The IPS Signatures Viewer table appears, by default, at the bottom of the page; however, you can choose to hide the table or position the table at the right side of the page.



If virtual domains are enabled on the unit, the Intrusion Protection settings are configured separately in each VDOM. All sensors and custom signatures will appear only in the VDOM in which they were created.

Predefined page

Lists each predefined signature that is currently on your unit. When you select the name of the signature, you are automatically redirected to that signature's detailed definition in the FortiGuard Center Vulnerability Encyclopedia. This page also indicates which signatures are enabled and which are disabled.

Tip: To determine what effect IPS protection will have on your network traffic, enable the required signatures, set the *Action* to *Pass*, and enable logging. Traffic will not be interrupted, and you will be able to examine, in detail, which signatures were detected.

Tags	<p>Select to add or remove tags to the predefined signature.</p> <p>Note: If tag settings are not available on the web-based manager, they must be enabled in <i>System > Admin > Settings</i> to then appear on the Predefined page.</p> <p>When you select the down arrow beside <i>Tags</i>, you can add tags or remove tags.</p> <p>To add tags to a predefined signature, select the signature first, select the down arrow beside <i>Tags</i>, and then select <i>Add Tags</i>. The Add Tags window appears. Enter the tag in the <i>Add Tag</i> field and then select the plus (+) sign; repeat until all tags are in the <i>Tags to apply</i> list.</p> <p>To remove tags, select the signature first, select the down arrow beside <i>Tags</i>, and then select <i>Remove Tags</i>. The Remove Tags window appears. Select the tags that you want removed in the <i>Applied Tags</i> row; repeat until all the tags are in the <i>Tags to remove</i> row. The tags will automatically be put in the <i>Tags to remove</i> row after being selected in the <i>Applied Tags</i> row.</p> <p>Note: When you select a signature, the Signature Viewer Table appears. The Signature Viewer Table is the same as the Log Viewer Table, providing detailed information about a signature.</p> <p>If there are tags that you want to add that have been configured for another object, you can add those tags as well to signatures. To apply these other object tags, select the signature first, select the down arrow beside <i>Tags</i>, and then select <i>Add Tags</i>. The Add Tags window appears. Select the tags you want to add in the <i>Click tag to add</i> row. The tags automatically appear in the <i>Tags to apply</i> row. Select <i>OK</i> to add those tags to the application.</p>
Column Settings	<p>Select to customize the signature information displayed in the table. You can also readjust the column order.</p>

Filter Settings	<p>Select to filter the information on the page. <i>Filters</i> appears automatically after selecting <i>Filter Settings</i>, below the column headings. Use to configure filter settings.</p> <p>Note: <i>Filter Settings</i> configures all filter settings. Filter icons are used to configure filter settings within that column.</p> <p>To apply a filter setting, select the plus sign beside <i>Add new filter</i> and then select and enter the information required. Repeat to add other filter settings. To modify settings, select <i>Change</i> beside the setting and edit the settings.</p> <p>To clear all filter settings, select the icon beside <i>Clear all filters</i>.</p> <p>To use a filter icon to filter settings within a column, select the filter icon in the column; <i>Filters</i> appears. Within <i>Filters</i>, configure the settings for that column.</p> <p>The <i>Filters Settings</i> on the <i>Predefined</i> page contains <i>Copy to Sensor</i>, which allows you to copy filter settings and apply them to a IPS sensor.</p> <p>To apply existing filter settings to a sensor, select the down arrow beside <i>Filter Settings</i>, and then select <i>Copy to Sensor</i>. The <i>Select Object</i> window appears. Select the sensor that you want to apply the settings to from the drop-down list. Select <i>OK</i>.</p>
View Details	Select the down arrow to choose to either hide the predefined signature viewer table or position the table on the right side of the page.
Search	Enter search criteria in the field provided. Select the <i>Clear All</i> icon beside the field to clear the criteria for a new search.
Name	The name of the signature. Each name is also a link to the description of the signature in the FortiGuard Center Vulnerability Encyclopedia .
Severity	The severity rating of the signature. The severity levels, from lowest to highest, are <i>Information</i> , <i>Low</i> , <i>Medium</i> , <i>High</i> , and <i>Critical</i> . These levels appear as bars in this column; each bar is explained in the predefined signature viewer table.
Target	The target of the signature: servers, clients, or both.
Protocols	The protocol the signature applies to.
OS	The operating system the signature applies to.
Applications	The applications the signature applies to.
Tags	The tags that are applied to the predefined signature.
Enable	The default status of the signature. A green check mark indicates the signature is enabled. A gray x indicates the signature is not enabled.
Action	<p>The default action for the signature:</p> <ul style="list-style-type: none"> • <i>Pass</i> – allows the traffic to continue without any modification. • <i>Drop</i> – prevents the traffic with detected signatures from reaching its destination. <p>If logging is enabled, the action appears in the status field of the log message generated by the signature.</p>
Page Controls	Use to navigate through the list on the page.

Custom

Custom signatures provide the power and flexibility to customize the Intrusion Protection system for diverse network environments. The predefined signatures represent common attacks. If you use an unusual or specialized application or an uncommon platform, you can add custom signatures based on the security alerts released by the application and platform vendors.

You can also create custom signatures to help you block P2P protocols.

After creating custom signatures, you need to specify them in IPS sensors that were created to scan traffic.

Use custom signatures to block or allow specific traffic. For example, to block traffic containing profanity, add custom signatures similar to the following:

```
set signature 'F-SBID (--protocol tcp; --flow bi_direction; --
pattern "bad words"; --no_case) '
```

Custom signatures must be added to a signature override in an IPS filter to have any effect. Creating a custom signature is a necessary step, but a custom signature does not affect traffic simply by being created.



Custom signatures are an advanced feature. This document assumes the user has previous experience creating intrusion detection signatures.

Custom signature configuration settings

The following are custom signature configuration settings in *UTM Profiles > Intrusion Protection > Custom*.



If virtual domains are enabled on the unit, the Intrusion Protection settings are configured separately in each VDOM. All sensors and custom signatures will appear only in the VDOM in which they were created.

Custom page

Lists each custom signature that you created. On this page you can edit, delete or create a new custom signature.

Create New	Creates a new custom signature. When you select <i>Create New</i> , you are automatically redirected to the New Custom Signature page.
Edit	Modifies the name or signature of a custom signature. When you select <i>Edit</i> , you are automatically redirected to the Edit Custom Signature page.
Delete	Removes a custom signature from the list on the Custom page. To remove multiple custom signatures from within the list, on the Custom page, in each of the rows of the custom signatures you want removed, select the check box and then select <i>Delete</i> . To remove all custom signatures from the list, on the Custom page, select the check box in the check box column and then select <i>Delete</i> .
Name	The name of the custom signature.
Signature	The signature itself.

New Custom Signature page

Provides settings for configuring a new custom signature.

Name	Enter a name for the custom signature.
Signature	Enter the signature.

Protocol Decoder

The Intrusion Protection system uses protocol decoders to identify the abnormal traffic patterns that do not meet the protocol requirements and standards. For example, the HTTP decoder monitors traffic to identify any HTTP packets that do not meet the HTTP protocol standards.

The decoder list is provided for your reference and can be configured using the CLI.

You can view protocol decoders in *UTM Profiles > Intrusion Protection > Protocol Decoder*.

Protocol Decoder page

Displays a list of the current protocol decoders that are on your unit. The unit automatically updates this list by contacting the FDN. This lists includes the port number that the protocol decoder monitors.

Protocols	The protocol decoder name.
Ports	The port number or numbers that the decoder monitors.

Upgrading the IPS protocol decoder list

The Intrusion Protection system protocol decoders are upgraded automatically through the FortiGuard Distribution Network (FDN) if existing decoders are modified or new decoders added. The FDN keeps the protocol decoder list up-to-date with protection against new threats such as the latest versions of existing IM/P2P as well as against new applications.



Web filter

This section describes FortiGate web filtering for HTTP traffic. The three main parts of the web filtering function, the Web Content Filter, the URL Filter, and the FortiGuard Web Filtering Service interact with each other to provide maximum control over what the Internet user can view as well as protection to your network from many Internet content threats. Web Content Filter blocks web pages containing words or patterns that you specify. URL filtering uses URLs and URL patterns to block or exempt web pages from specific sources. FortiGuard Web Filtering provides many additional categories you can use to filter web traffic.

Before you begin

Before you follow the instructions in this section, you should have a FortiGuard Web Filter subscription and your FortiGate unit should be properly configured to communicate with the FortiGuard servers.

This section describes the Web Content Filter and URL Filter functions. For information on FortiGuard Web Filtering, see [“FortiGuard Web Filter” on page 159](#).

The following topics are included in this section:

- [Web filter concepts](#)
- [Web content filter](#)
- [URL filter](#)
- [SafeSearch](#)
- [Advanced web filter configuration](#)
- [Web filtering example](#)

Web filter concepts

Web filtering is a means of controlling the content that an Internet user is able to view. With the popularity of web applications, the need to monitor and control web access is becoming a key component of secure content management systems that employ antivirus, web filtering, and messaging security. Important reasons for controlling web content include:

- lost productivity because employees are accessing the web for non-business reasons
- network congestion — when valuable bandwidth is used for non-business purposes, legitimate business applications suffer
- loss or exposure of confidential information through chat sites, non-approved email systems, instant messaging, and peer-to-peer file sharing
- increased exposure to web-based threats as employees surf non-business-related web sites
- legal liability when employees access/download inappropriate and offensive material
- copyright infringement caused by employees downloading and/or distributing copyrighted material.

As the number and severity of threats increase on the World Wide Web, the risk potential increases within a company's network as well. Casual non-business related web surfing has caused many businesses countless hours of legal litigation as hostile environments have been created by employees who download and view offensive content. Web-based attacks and threats are also becoming increasingly sophisticated. Threats and web-based applications that cause additional problems for corporations include:

- spyware/grayware
- phishing
- pharming
- instant messaging
- peer-to-peer file sharing
- streaming media
- blended network attacks.

Spyware, also known as grayware, is a type of computer program that attaches itself to a user's operating system. It does this without the user's consent or knowledge. It usually ends up on a computer because of something the user does such as clicking on a button in a pop-up window. Spyware can track the user's Internet usage, cause unwanted pop-up windows, and even direct the user to a host web site. For further information, visit the [FortiGuard Center](#).

Some of the most common ways of grayware infection include:

- downloading shareware, freeware, or other forms of file-sharing services
- clicking on pop-up advertising
- visiting legitimate web sites infected with grayware.

Phishing is the term used to describe attacks that use web technology to trick users into revealing personal or financial information. Phishing attacks use web sites and email that claim to be from legitimate financial institutions to trick the viewer into believing that they are legitimate. Although phishing is initiated by spam email, getting the user to access the attacker's web site is always the next step.

Pharming is a next generation threat that is designed to identify and extract financial, and other key pieces of information for identity theft. Pharming is much more dangerous than phishing because it is designed to be completely hidden from the end user. Unlike phishing attacks that send out spam email requiring the user to click to a fraudulent URL, pharming attacks require no action from the user outside of their regular web surfing activities. Pharming attacks succeed by redirecting users from legitimate web sites to similar fraudulent web sites that have been created to look and feel like the authentic web site.

Instant messaging presents a number of problems. Instant messaging can be used to infect computers with spyware and viruses. Phishing attacks can be made using instant messaging. There is also a danger that employees may use instant messaging to release sensitive information to an outsider.

Peer-to-peer (P2P) networks are used for file sharing. Such files may contain viruses. Peer-to-peer applications take up valuable network resources and may lower employee productivity but also have legal implications with the downloading of copyrighted or sensitive company material.

Streaming media is a method of delivering multimedia, usually in the form of audio or video to Internet users. Viewing streaming media impacts legitimate business by using valuable bandwidth.

Blended network threats are rising and the sophistication of network threats is increasing with each new attack. Attackers learn from each previous successful attack and enhance and update attack code to become more dangerous and fast spreading. Blended attacks use a combination of methods to spread and cause damage. Using virus or network worm techniques combined with known system vulnerabilities, blended threats can quickly spread through email, web sites, and Trojan applications. Examples of blended threats include Nimda, Code Red, Slammer, and Blaster. Blended attacks can be designed to perform different types of attacks, which include disrupting network services, destroying or stealing information, and installing stealthy backdoor applications to grant remote access.

Different ways of controlling access

The methods available for monitoring and controlling Internet access range from manual and educational methods to fully automated systems designed to scan, inspect, rate and control web activity.

Common web access control mechanisms include:

- establishing and implementing a well-written usage policy in the organization on proper Internet, email, and computer conduct
- installing monitoring tools that record and report on Internet usage
- implementing policy-based tools that capture, rate, and block URLs.

The final method is the focus of this topic. The following information shows how the filters interact and how to use them to your advantage.

Order of web filtering

The FortiGate unit applies web filters in a specific order:

- 1 URL filter
- 2 FortiGuard Web Filter
- 3 web content filter
- 4 web script filter
- 5 antivirus scanning.

If you have blocked a FortiGuard Web Filter category but want certain users to have access to URLs within that pattern, you can use the *Override* within the FortiGuard Web Filter. This will allow you to specify which users have access to which blocked URLs and how long they have that access. For example, if you want a user to be able to access www.example.com for one hour, you can use the override to set up the exemption. Any user listed in an override must fill out an online authentication form that is presented when they try to access a blocked URL before the FortiGate unit will grant access to it. For more information, see [“FortiGuard Web Filter” on page 159](#).

Web content filter

You can control web content by blocking access to web pages containing specific words or patterns. This helps to prevent access to pages with questionable material. You can also add words, phrases, patterns, wild cards and Perl regular expressions to match content on web pages. You can add multiple web content filter lists and then select the best web content filter list for each web filter profile.

Enabling web content filtering involves three separate parts of the FortiGate configuration.

- The security policy allows certain network traffic based on the sender, receiver, interface, traffic type, and time of day.
- The web filter profile specifies what sort of web filtering is applied.
- The web content filter list contains blocked and exempt patterns.

The web content filter feature scans the content of every web page that is accepted by a security policy. The system administrator can specify banned words and phrases and attach a numerical value, or score, to the importance of those words and phrases. When the web content filter scan detects banned content, it adds the scores of banned words and phrases in the page. If the sum is higher than a threshold set in the web filter profile, the FortiGate unit blocks the page.

General configuration steps

Follow the configuration procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

- 1 Create a web content filter list.
- 2 Add patterns of words, phrases, wildcards, and regular expressions that match the content to be blocked or exempted.

You can add the patterns in any order to the list. You need to add at least one pattern that blocks content.
- 3 In a web filter profile, enable the web content filter and select a web content filter list from the options list.

To complete the configuration, you need to select a security policy or create a new one. Then, in the security policy, enable *UTM* and select the appropriate web filter profile from the list.

Creating a web filter content list

You can create multiple content lists and then select the best one for each web filter profile. Creating your own web content lists can be accomplished only using the CLI.

This example shows how to create a web content list called inappropriate language, with two entries, offensive and rude.

To create a web filter content list

```
config webfilter content
edit 3
set name "inappropriate language"
config entries
edit offensive
set action block
set lang western
set pattern-type wildcard
set score 15
set status enable
next
edit rude
set action block
set lang western
set pattern-type wildcard
set score 5
set status enable
end
```



```

end
end

```

See the [CLI Reference](#) for a complete description of all the web filter content list commands and options.

How content is evaluated

Every time the web content filter detects banned content on a web page, it adds the score for that content to the sum of scores for that web page. You set this score when you create a new pattern to block the content. The score can be any number from zero to 99999. Higher scores indicate more offensive content. When the sum of scores equals or exceeds the threshold score, the web page is blocked. The default score for web content filter is 10 and the default threshold is 10. This means that by default a web page is blocked by a single match. Blocked pages are replaced with a message indicating that the page is not accessible according to the Internet usage policy.

Banned words or phrases are evaluated according to the following rules:

- The score for each word or phrase is counted only once, even if that word or phrase appears many times in the web page.
- The score for any word in a phrase without quotation marks is counted.
- The score for a phrase in quotation marks is counted only if it appears exactly as written.

The following table describes how these rules are applied to the contents of a web page. Consider the following, a web page that contains only this sentence: “The score for each word or phrase is counted only once, even if that word or phrase appears many times in the web page.”

Table 13: Banned Pattern Rules

Banned pattern	Assigned score	Score added to the sum for the entire page	Threshold score	Comment
word	20	20	20	Appears twice but only counted once. Web page is blocked.
word phrase	20	40	20	Each word appears twice but only counted once giving a total score of 40. Web page is blocked
word sentence	20	20	20	“word” appears twice, “sentence” does not appear, but since any word in a phrase without quotation marks is counted, the score for this pattern is 20. Web page is blocked.

Table 13: Banned Pattern Rules (Continued)

Banned pattern	Assigned score	Score added to the sum for the entire page	Threshold score	Comment
"word sentence"	20	0	20	"This phrase does not appear exactly as written. Web page is allowed.
"word or phrase"	20	20	20	This phrase appears twice but is counted only once. Web page is blocked.

Enabling the web content filter and setting the content threshold

When you enable the web content filter, the web filter will block any web pages when the sum of scores for banned content on that page exceeds the content block threshold. The threshold will be disregarded for any exemptions within the web filter list.

To enable the web content filter and set the content block threshold

- 1 Go to *UTM Profiles > Web Filter > Profile*.
- 2 Select the *Create New* icon on the Edit Web Filter Profile window title bar.
- 3 In the *Name* field, enter the name of the new web filter profile.
- 4 Optionally, you may also enter a comment. The comment can remind you of the details of the sensor.
- 5 Select the *Inspection Method*.
 Proxy-based detection involves buffering the file and examining it as a whole. Advantages of proxy-based detection include a more thorough examination of attachments, especially archive formats and nesting.
 Flow-based detection examines the file as it passes through the FortiGate unit without any buffering. Advantages of flow-based detection include speed and no interruption of detection during conserve mode.
- 6 Expand the *Advanced Filter* heading.
- 7 Enable *Web Content Filter*.
- 8 Select the required web filter content list from the *Web Content Filter* drop-down list.
- 9 Enter a threshold value.
- 10 Select *Apply*.

The web filter profile configured with web content filtering is ready to be added to a firewall profile.

URL filter

You can allow or block access to specific URLs by adding them to the URL filter list. You add the URLs by using patterns containing text and regular expressions. The FortiGate unit allows or blocks web pages matching any specified URLs or patterns and displays a replacement message instead.



URL blocking does not block access to other services that users can access with a web browser. For example, URL blocking does not block access to ftp://ftp.example.com. Instead, use firewall policies to deny ftp connections.

When adding a URL to the URL filter list, follow these rules:

- Type a top-level URL or IP address to control access to all pages on a web site. For example, `www.example.com` or `192.168.144.155` controls access to all pages at this web site.
- Enter a top-level URL followed by the path and file name to control access to a single page on a web site. For example, `www.example.com/news.html` or `192.168.144.155/news.html` controls access to the news page on this web site.
- To control access to all pages with a URL that ends with `example.com`, add `example.com` to the filter list. For example, adding `example.com` controls access to `www.example.com`, `mail.example.com`, `www.finance.example.com`, and so on.
- Control access to all URLs that match patterns using text and regular expressions (or wildcard characters). For example, `example.*` matches `example.com`, `example.org`, `example.net` and so on.



URLs with an action set to exempt or pass are not scanned for viruses. If users on the network download files through the FortiGate unit from a trusted web site, add the URL of this web site to the URL filter list with an action to pass it so the FortiGate unit does not virus scan files downloaded from this URL.

URL filter actions

You can select one of four actions for URL patterns you include in URL filter lists.

Block

Attempts to access any URLs matching the URL pattern are denied. The user will be presented with a replacement message.

Allow

Any attempt to access a URL that matches a URL pattern with an allow action is permitted. The traffic is passed to the remaining antivirus proxy operations, including FortiGuard Web Filter, web content filter, web script filters, and antivirus scanning.

Allow is the default action. If a URL does not appear in the URL list, it is permitted.

Monitor

Traffic to, and reply traffic from, sites matching a URL pattern with a monitor be allowed through in the same way as the “Allow” action. The difference with the Monitor action being that a log message will be generated each time a matching traffic session is established. The requests will also be subject to all other UTM inspections that would normally be applied to the traffic.

Exempt

Exempt allows trusted traffic to bypass the antivirus proxy operations.

HTTP 1.1 connections are persistent unless declared otherwise. This means the connections will remain in place until closed or the connection times out. When a client loads a web page, the client opens a connection to the web server. If the client follows a link to another page on the same site before the connection times out, the same connection is used to request and receive the page data.

When you add a URL pattern to a URL filter list and apply the Exempt action, traffic sent to and replies traffic from sites matching the URL pattern will bypass all antivirus proxy operations. The connection itself inherits the exemption. This means that all subsequent reuse of the existing connection will also bypass all antivirus proxy operations. When the connection times out, the exemption is cancelled.

For example, consider a URL filter list that includes `example.com/files` configured with the Exempt action. A user opens a web browser and downloads a file from the URL `example.com/sample.zip`. This URL does not match the URL pattern so it is scanned for viruses. The user then downloads `example.com/files/beautiful.exe` and since this URL does match the pattern, the connection itself inherits the exempt action. The user then downloads `example.com/virus.zip`. Although this URL does not match the exempt URL pattern, a previously visited URL did, and since the connection inherited the exempt action and was re-used to download a file, the file is not scanned.

If the user next goes to an entirely different server, like `example.org/photos`, the connection to the current server cannot be reused. A new connection to `example.org` is established. This connection is not exempt. Unless the user goes back to `example.com` before the connection to that server times out, the server will close the connection. If the user returns after the connection is closed, a new connection to `example.com` is created and it is not exempt until the user visits a URL that matches the URL pattern.

Web servers typically have short time-out periods. A browser will download multiple components of a web page as quickly as possible by opening multiple connections. A web page that includes three photos will load more quickly if the browser opens four connections to the server and downloads the page and the three photos at the same time. A short time-out period on the connections will close the connections faster, allowing the server to avoid unnecessarily allocating resources for a long period. The HTTP session time-out is set by the server and will vary with the server software, version, and configuration.

Using the exempt action can have unintended consequences in certain circumstances. You have a web site at `example.com` and since you control the site, you trust the contents and configure `example.com` as exempt. But `example.com` is hosted on a shared server with a dozen other different sites, each with a unique domain name. Because of the shared hosting, they also share the same IP address. If you visit `example.com`, your connection your site becomes exempt from any antivirus proxy operations. Visits to any of the 12 other sites on the same server will reuse the same connection and the data you receive is exempt from scanned.

Use of the exempt action is not suitable for configuration in which connections through the FortiGate unit use an external proxy. For example, you use `proxy.example.net` for all outgoing web access. Also, as in the first example, URL filter list that includes a URL pattern of `example.com/files` configured with the Exempt action. Users are protected by the antivirus protection of the FortiGate unit until a user visits a URL that matches the `example.com/files` URL pattern. The pattern is configured with the Exempt action so the connection to the server inherits the exemption. With a proxy however, the connection is from the user to the proxy. Therefore, the user is entirely unprotected until the connection times out, no matter what site he visits.

Ensure you are aware of the network topology involving any URLs to which you apply the Exempt action.

General configuration steps

Follow the configuration procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

- 1 Create a URL filter list.
- 2 Add URLs to the URL filter list.
- 3 Select a web filter profile or create a new one.
- 4 In the web filter profile, create a URL List filter.

To complete the configuration, you need to select a security policy or create a new one. Then, in the security policy, enable *UTM* and select the appropriate web filter profile from the list.

Creating a URL filter list

To create a URL Filter list

- 1 Go to *UTM Profiles > Web Filter > URL Filter*.
- 2 Select *Create New*.
- 3 Enter a *Name* for the new URL filter list.
- 4 Enter optional comments to describe it.
- 5 Select *OK*.

Configuring a URL filter list

Each URL filter list can have up to 5000 entries. For this example, the URL `www.example*.com` will be used. You configure the list by adding one or more URLs to it.

To add a URL to a URL filter list

- 1 Go to *UTM Profiles > Web Filter > URL Filter*.
- 2 Select an existing list and choose *Edit*.
- 3 Select *Create New*.
- 4 Enter the URL, without the “http”, for example: `www.example*.com`.
- 5 Select a *Type*: *Simple*, *Wildcard* or *Regular Expression*.
In this example, select *Wildcard*.
- 6 Select the *Action* to take against matching URLs: *Exempt*, *Block*, *Allow*, or *Monitor*.
- 7 Select *Enable*.
- 8 Select *OK*.

SafeSearch

SafeSearch is a feature of popular search sites that prevents explicit web sites and images from appearing in search results. Although SafeSearch is a useful tool, especially in educational environments, the resourceful user may be able to simply turn it off. Enabling SafeSearch for the supported search sites enforces its use by rewriting the search URL to include the code to indicate the use of the SafeSearch feature.

Three search sites are supported:

Google	Enforce the strict filtering level of safe search protection for Google search results by adding <code>&safe=on</code> to search URL requests. Strict filtering removes both explicit text and explicit images from the search results.
Yahoo!	Enforce the strict filtering level of safe search protection for Yahoo! search results by adding <code>&vm=r</code> to search URL requests. Strict filtering removed adult web, video, and images from search results.
Bing	Enforce the strict filtering level of safe search protection for Bing search results by adding <code>adlt=strict</code> to search URL requests. Strict filtering removes explicit text, images, and video from the search results.

Enabling SafeSearch – CLI

```
config webfilter profile
  edit default
    config web
      set safe-search bing google yahoo
    end
  end
```

This enforces the use of SafeSearch in traffic controlled by the firewall policies using the web filter you configure.

Advanced web filter configuration

The *Advanced Filter* section of the web filter profile provides a number of advanced filtering options. The FortiGuard Web Filter options in the advance filter section are detailed in the FortiGuard Web Filter section, in [“Advanced FortiGuard Web Filter configuration” on page 165](#).

ActiveX filter

Enable to filter ActiveX scripts from web traffic. Web sites using ActiveX may not function properly with this filter enabled.

Cookie filter

Enable to filter cookies from web traffic. Web sites using cookies may not function properly with this enabled.

Java applet filter

Enable to filter java applets from web traffic. Web sites using java applets may not function properly with this filter enabled.

Web resume download block

Enable to prevent the resumption of a file download where it was previously interrupted. With this filter enabled, any attempt to restart an aborted download will download the file from the beginning rather than resuming from where it left off.

This prevents the unintentional download of viruses hidden in fragmented files.

Note that some types of files, such as PDF, fragment files to increase download speed and enabling this option can cause download interruptions. Enabling this option may also break certain applications that use the Range Header in the HTTP protocol, such as YUM, a Linux update manager.

Block Invalid URLs

Select to block web sites when their SSL certificate CN field does not contain a valid domain name.

FortiGate units always validate the CN field, regardless of whether this option is enabled. However, if this option is not selected, the following behavior occurs:

- If the request is made directly to the web server, rather than a web server proxy, the FortiGate unit queries for FortiGuard Web Filtering category or class ratings using the IP address only, not the domain name.
- If the request is to a web server proxy, the real IP address of the web server is not known. Therefore, rating queries by either or both the IP address and the domain name is not reliable. In this case, the FortiGate unit does not perform FortiGuard Web Filtering.

HTTP POST action

Select the action to take with HTTP POST traffic. HTTP POST is the command used by your browser when you send information, such as a form you have filled-out or a file you are uploading, to a web server.

The available actions include:

Normal	Allow use of the HTTP POST command as normal.
Comfort	Use client comforting to slowly send data to the web server as the FortiGate unit scans the file. Use this option to prevent a server time-out when scanning or other filtering is enabled for outgoing traffic. The client comforting settings used are those defined in the protocol options profile selected in the security policy. For more information, see “Configuring client comforting” on page 40 .
Block	Block the HTTP POST command. This will limit users from sending information and files to web sites. When the post request is blocked, the FortiGate unit sends the http-post-block replacement message to the web browser attempting to use the command.

Web filtering example

Web filtering is particularly important for protecting school-aged children. There are legal issues associated with improper web filtering as well as a moral responsibility not to allow children to view inappropriate material. The key is to design a web filtering system in such a way that students and staff do not fall under the same web filter profile in the FortiGate configuration. This is important because the staff may need to access websites that are off-limits to the students.

School district

The background for this scenario is a school district with more than 2300 students and 500 faculty and staff in a preschool, three elementary schools, a middle school, a high school, and a continuing education center. Each elementary school has a computer lab and the high school has three computer labs with connections to the Internet. Such easy access to the Internet ensures that every student touches a computer every day.

With such a diverse group of Internet users, it was not possible for the school district to set different Internet access levels. This meant that faculty and staff were unable to view websites that the school district had blocked. Another issue was the students' use of proxy sites to circumvent the previous web filtering system. A proxy server acts as a go-between for users seeking to view web pages from another server. If the proxy server has not been blocked by the school district, the students can access the blocked website.

When determining what websites are appropriate for each school, the district examined a number of factors, such as community standards and different needs of each school based on the age of the students.

The district decided to configure the FortiGate web filtering options to block content of an inappropriate nature and to allow each individual school to modify the options to suit the age of the students. This way, each individual school was able to add or remove blocked sites almost immediately and have greater control over their students' Internet usage.

In this simplified example of the scenario, the district wants to block any websites with the word **example** on them, as well as the website `www.example.com`. The first task is to create web content filter lists for the students and the teachers.

To create a web content filter list for the students

```
config webfilter content
  edit 5
    set name "Student Web Content List"
    config entries
      edit example
        set action block
        set status enable
      end
    end
  end
```

It might be more efficient if the Teacher Web Content List included the same blocked content as the student list. From time to time a teacher might have to view a blocked page. It would then be a matter of changing the *Action* from *Block* to *Allow* as the situation required.

To create a web content filter list for the teachers

```
config webfilter content
  edit 5
    set name "Teacher Web Content List"
    config entries
      edit example
        set action exempt
        set status enable
      end
    end
  end
```

URL filter lists with filters to block unwanted web sites must be created for the students and teachers. For this example the URL `www.example.com` will be used.

To create a URL filter for the students

- 1 Go to *UTM Profiles > Web Filter > URL Filter*.
- 2 Select *Create New*.
- 3 Enter `Student URL List` as the URL filter *Name*.
- 4 Enter optional comments to describe the contents of the list.
- 5 Select *OK*.
The URL filter for the students has been created. Now it must be configured.
- 6 Select *Create New*.
- 7 Enter `example.com` in the URL field.
- 8 Select *Simple* from the *Type* list.
- 9 Select *Block* from the *Action* list.
- 10 Select *Enable*.
- 11 Select *OK*.
- 12 Select *OK*.

The teachers should be able to view the students' blocked content, however, so an addition URL filter is needed.

To create a URL filter for the teachers

- 1 Go to *UTM Profiles > Web Filter > URL Filter*.
- 2 Select *Create New*.
- 3 Enter `Teacher URL List` as the URL filter *Name*.
- 4 Enter optional comments to describe the list.
- 5 Select *OK*.
The URL filter for the students has been created. Now it must be configured.
- 6 Select *Create New*.
- 7 Enter `www.example.com` in the *URL* field.
- 8 Select *Simple* from the *Type* list.
- 9 Select *Exempt* from the *Action* list.
- 10 Select *Enable*.
- 11 Select *OK*.
- 12 Select *OK*.

A web filter profile must be created for the students and the teachers.

To create a web filter profile for the students

- 1 Go to *UTM Profiles > Web Filter > Profile*.
- 2 Select the *Create New* icon in the Edit Web Filter window title bar.
- 3 Enter `Students` as the *Profile Name*.
- 4 Enter optional comments to identify the profile.
- 5 Expand the *Advanced Filter* heading.
- 6 Enable *Web Content Filter*.
- 7 Select *Student Web Content List* from the *Web Content Filter* drop-down list.
- 8 Enable *Web URL Filter*.

9 Select *Student URL List* from the *Web URL Filter* drop-down list.

10 Enable *Web Resume Download Block*.

Selecting this setting will block downloading parts of a file that have already been downloaded and prevent the unintentional download of virus files hidden in fragmented files. Note that some types of files, such as PDFs, are fragmented to increase download speed, and that selecting this option can cause download interruptions with these types.

11 Select *OK*.

To create a security policy for the students

1 Go to *Policy > Policy > Policy*.

2 Select *Create New*.

3 Enable *UTM*.

4 Select *Enable Web Filter*.

5 Select *Students* from the web filter drop-down list.

6 Enter optional comments.

7 Select *OK*.

To create a web filter profile for the teachers

1 Go to *UTM Profiles > Web Filter > Profile*.

2 Select the *Create New* icon in the Edit Web Filter window title bar.

3 Enter *Teachers* as the *Profile Name*.

4 Enter optional comments to identify the profile.

5 Expand the *Advanced Filter* heading.

6 Enable *Web Content Filter*.

7 Select *Teacher Web Content List* from the *Web Content Filter* drop-down list.

8 Enable *Web URL Filter*.

9 Select *Teacher URL List* from the *Web URL Filter* drop-down list.

10 Enable *Web Resume Download Block*.

11 Select *OK*.

To create a security policy for Teachers

1 Go to *Policy > Policy > Policy*.

2 Select *Create New*.

3 Enable *UTM*.

4 Select *Enable Web Filter*.

5 Select *Teachers* from the web filter drop-down list.

6 Enter optional comments.

7 Select *OK*.

Web Filter interface reference

The following explains the web filtering options in the Web Filtering menu. If your unit supports SSL content scanning and inspection you can also configure web filtering for HTTPS traffic.

If you want to configure advanced settings, such as web content filter, you must configure them within the CLI. Advanced settings also includes overrides.

This topic includes the following:

- [Profile](#)
- [Browser cookie-based FortiGuard Web Filtering overrides](#)
- [URL Filter](#)
- [Local Ratings](#)

Profile

The Profile menu allows you to configure a web filter profile to apply to a firewall policy. A profile is specific information that defines how the traffic within a policy is examined and what action may be taken based on the examination.

Web profile configuration settings

The following are web filter profile configuration settings in *UTM Profiles > Web Filter > Profile*. If you want to configure advanced settings, such as FortiGuard web filtering overrides, you must configure these settings within the CLI.

Profile page Lists each web filter profile that you created. On this page, you can edit, delete or create a new web filter profile. You are redirected to this page when you select <i>View List</i> on the Edit Web Filter Profile page. Note: Web filtering overrides are profile-based, allowing a rule to be created that changes the web filter profile that applies to a user. An override link appears in all related blocked pages. This is available only in the CLI.	
Create New	Creates a new web filter profile. When you select <i>Create New</i> , you are automatically redirected to the New Web Filter Profile page.
Edit	Modifies settings within a web filter profile. When you select <i>Edit</i> , you are automatically redirected to the Edit Web Filter Profile page.
Delete	Removes a web filter profile from within the list on the Profile page. To remove multiple web filter profiles from within the list, on the Profile page, in each of the rows of the file filter lists you want removed, select the check box and then select <i>Delete</i> . To remove all web filter profiles from the list, on the Profile page, select the check box in the check box column and then select <i>Delete</i> .
Name	The name of the web filter profile.
Comments	A description given to the web filter profile. This is an optional setting.

Ref.	<p>Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a firewall policy; on the Profile page (<i>UTM Profiles > Antivirus > Profile</i>), 1 appears in <i>Ref.</i>.</p> <p>To view the location of the referenced object, select the number in <i>Ref.</i>, and the Object Usage window appears displaying the various locations of the referenced object.</p> <p>To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:</p> <ul style="list-style-type: none"> • View the list page for these objects – automatically redirects you to the list page where the object is referenced at. • Edit this object – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • View the details for this object – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy, and that firewall policy's settings appear within the table.
<p>New Web Filter Profile page</p> <p>Provides settings for configuring a web filter profile. Advanced features, such as web content filtering and FortiGuard web filtering, is configured in the CLI.</p> <p>This page appears when you select <i>Create New</i> on the Edit Web Filter Profile page. If you are on the Profile page, and you select <i>Create New</i>, you will be redirected to the New Web Filter Profile page.</p> <p>Note: Logging is enabled in the CLI.</p>	
Name	<p>Enter a name for the web filter profile.</p> <p>If you want to edit the name at any time, select the profile and enter a new name in the <i>Name</i> field. Select <i>Apply</i> to save the change.</p>
Comments	<p>Enter a description for the web filter profile. This is optional.</p> <p>If you want to edit the description at any time, select the profile and enter the new description in the <i>Comments</i> field. Select <i>Apply</i> to save the change.</p>
Inspection mode	<p>Select to enable either flow-based web filtering or proxy-based.</p> <p>Flow-based web filtering is a non-proxy solution, which provides high concurrent session, high session rate, and low-latency web filtering service.</p>

FortiGuard Categories	A list of FortiGuard category groups and categories that are used to rate web sites. Selecting a category group will automatically select all of the categories within the group. For example, if you select Security Risk, you can see that all of the categories within are selected if you expand the group. You can however, select or deselect categories within groups as required.
Show	Select an action to view all of the categories that are currently configured with the selected action.
Change Action for Selected Categories to	Select an action, and all of the selected categories will have the selected action applied. Selected category groups will have the action applied to all categories within the group.
Quota on Categories	<p>Users can have their web browsing time limited by category through the use of quotas. Quotas can be applied only to categories that are configured with the Monitor action.</p> <p>If you create a quota for a single category, every authenticated user subject to the security policy in which the web filter profile is applied is limited in browsing web sites in the category to the duration you specify. If you create a single quota that includes multiple categories, the quota will apply to the categories as a whole.</p> <p>Quotas are ignored for unauthenticated users. To enforce quotas, configure the security policy to require authentication.</p>
Enable Safe Search (Support Search Engines: Google, Yahoo and Bing)	When enabled, the supported search engines exclude offensive material from search results.
HTTPS Scanning	<p>Available only on models that support HTTPS.</p> <p>Select to have all of the web filtering specified in the web filter profile to HTTPS traffic as well as HTTP traffic.</p>
Advanced Filter	Expand this heading for advanced web filtering options.
Web URL Filter	Enable to block access to URLs listed in the selected URL list.
Web Resume Download Block	<p>Enable to prevent the resumption of a file download where it was previously interrupted. With this filter enabled, any attempt to restart an aborted download will download the file from the beginning rather than resuming from where it left off.</p> <p>This prevents the unintentional download of viruses hidden in fragmented files.</p> <p>Note that some types of files, such as PDF, fragment files to increase download speed and enabling this option can cause download interruptions. Enabling this option may also break certain applications that use the Range Header in the HTTP protocol, such as YUM, a Linux update manager.</p>

Block Invalid URLs	<p>Select to block web sites when their SSL certificate CN field does not contain a valid domain name.</p> <p>FortiGate units always validate the CN field, regardless of whether this option is enabled. However, if this option is not selected, the following behavior occurs:</p> <ul style="list-style-type: none"> • If the request is made directly to the web server, rather than a web server proxy, the FortiGate unit queries for FortiGuard Web Filtering category or class ratings using the IP address only, not the domain name. • If the request is to a web server proxy, the real IP address of the web server is not known. Therefore, rating queries by either or both the IP address and the domain name is not reliable. In this case, the FortiGate unit does not perform FortiGuard Web Filtering.
HTTP POST Action	<p>Select the action to take with HTTP POST traffic. HTTP POST is the command used by your browser when you send information, such as a form you have filled-out or a file you are uploading, to a web server.</p> <p>The available actions include:</p> <ul style="list-style-type: none"> • Normal: Allow use of the HTTP POST command as normal. • Comfort: Use client comforting to slowly send data to the web server as the FortiGate unit scans the file. Use this option to prevent a server time-out when scanning or other filtering is enabled for outgoing traffic. The client comforting settings used are those defined in the protocol options profile selected in the security policy. • Block: Block the HTTP POST command. This will limit users from sending information and files to web sites. When the post request is blocked, the FortiGate unit sends the http-post-block replacement message to the web browser attempting to use the command.
Remove Java Applet Filter	Enable to filter java applets from web traffic. Web sites using java applets may not function properly with this filter enabled.
Remove ActiveX Filter	Enable to filter ActiveX scripts from web traffic. Web sites using ActiveX may not function properly with this filter enabled.
Remove Cookie Filter	Enable to filter cookies from web traffic. Web sites using cookies may not function properly with this enabled.
Search Engine Keyword Filter	Enter the keywords that you want to monitor when users enter those same or similar keywords during a search within the supported search engines.
Web Content Filter	Enable to block access to web pages that include the words included in the selected web content filter list.
Provide Details for Blocked HTTP 4xx and 5xx Errors	Enable to have the FortiGate unit display its own replacement message for 400 and 500-series HTTP errors. If the server error is allowed through, malicious or objectionable sites can use these common error pages to circumvent web filtering.

Rate Images by URL (Blocked images will be replaced with blanks)	<p>Enable to have the FortiGate retrieve ratings for individual images in addition to web sites. Images in a blocked category are not displayed even if they are part of a site in an allowed category.</p> <p>Blocked images are replaced on the originating web pages with blank place-holders. Rated image file types include GIF, JPEG, PNG, BMP, and TIFF.</p>
Allow Websites When a Rating Error Occurs	<p>Enable to allow access to web pages that return a rating error from the FortiGuard Web Filter service.</p> <p>If your FortiGate unit cannot contact the FortiGuard service temporarily, this setting determines what access the FortiGate unit allows until contact is re-established. If enabled, users will have full unfiltered access to all web sites. If disabled, users will not be allowed access to any web sites.</p>
Strict Blocking	<p>This setting determines when the FortiGate unit blocks a site. Enable strict blocking to deny access to a site if any category or classification assigned to the site is set to Block. Disable strict blocking to deny access to a site only if all categories and classifications assigned to the site are set to Block.</p> <p>All rated URLs are assigned one or more categories. URLs may also be assigned a classification. If Rate URLs by domain and IP address is enabled, the site URL and IP address each carry separately assigned categories and classifications. Depending on the FortiGuard rating and the FortiGate configuration, a site could be assigned to at least two categories and up to two classifications.</p>

<p>Rate URLs by Domain and IP Address</p>	<p>Enable to have the FortiGate unit request the rating of the site by URL and IP address separately, providing additional security against attempts to bypass the FortiGuard Web Filter.</p> <p>If the rating determined by the domain name and the rating determined by the IP address defer the Action that is enforce will be determined by a weighting assigned to the different categories. The higher weighted category will take precedence in determining the action. This will have the side effect that sometimes the Action will be determined by the classification based on the domain name and other times it will be determined by the classification that is based on the IP address.</p> <p>An example of how this would work would be if a URL's rating based on the domain name indicated that it belonged in the category Lingerie and Swimsuit, which is allowed but the category assigned to the IP address was Pornography which has an action of Block, because the Pornography category has a higher weight the effective action is Block.</p> <p>FortiGuard Web Filter ratings for IP addresses are not updated as quickly as ratings for URLs. This can sometimes cause the FortiGate unit to allow access to sites that should be blocked, or to block sites that should be allowed.</p>
<p>Block HTTP Redirects by Rating</p>	<p>Enable to block HTTP redirects.</p> <p>Many web sites use HTTP redirects legitimately but in some cases, redirects may be designed specifically to circumvent web filtering, as the initial web page could have a different rating than the destination web page of the redirect.</p> <p>This option is not supported for HTTPS.</p>

Browser cookie-based FortiGuard Web Filtering overrides

By using browser cookie-based FortiGuard Web Filtering overrides, you can identify users according to their web browser cookie instead of their IP address and then to use this identification to apply FortiGuard Web Filtering overrides to individual users.

This feature uses the dynamic profile feature to assign a web filter profile that includes FortiGuard Web Filtering to a communication session. Just like normal FortiGuard Web Filtering overrides, when FortiGuard Web Filtering blocks access to a web page, the user can authenticate to override FortiGuard Web Filtering. However, with Browser cookie-based overrides enabled, the browser cookie is used to identify the user instead of the user's IP address.

To allow browser based FortiGuard Web Filtering overrides in a user group, go to *User > User Group*, edit a firewall or directory service user group. Select *Allow to create FortiGuard Web Filtering overrides* and make sure *Browser (Cookie) Override* is set to *Allow*.

You can also go to *UTM Profiles > Web Filter > Configuration* and configure the following browser cookie-based override settings.



Additional browser cookie-based configuration settings are available from the CLI using the `config webfilter cookie-ovrd` command.

Cookie (Browser Based) Override Configuration page

Provides settings for configuring the browser cookie-based override.

Override Validation Hostname	Enter the override validation hostname in the field.
Override Validation Port	Enter the port number in the field.

How browser cookie-based FortiGuard Web Filtering overrides work

The following steps occur when a user's session that can use browser cookie-based FortiGuard Web Filtering overrides is received:

- 1 The Dynamic Profile applies a profile to the user session in the normal way.
- 2 The user issues a request to a remote site blocked by FortiGuard Web Filtering.
For example, <http://www.example.com>.
- 3 FortiGuard Web Filtering blocks the page and provides an override link.
- 4 The user selects the override option and successfully authenticates.
- 5 The unit sends a cookie to the remote site that seems to come from the *Override Validation Hostname*.
- 6 The unit creates a second cookie to the user's browser for the domain of the remote site.
For example, the domain could be example.com.

The rest of the communication between the user and the remote site is authorized with the unit by these cookies

URL Filter

Allow or block access to specific URLs by adding them to the URL filter list. Add patterns using text and regular expressions (or wildcard characters) to allow or block URLs. The unit allows or blocks web pages matching any specified URLs or patterns and displays a replacement message.

You can add multiple URL filter lists and then select the best URL filter list for each profile.

You can add the following to block or exempt URLs:

- complete URLs
- IP addresses
- partial URLs to allow or block all sub-domains

Each URL filter list can have up to 5000 entries.

URL filter configuration settings

The following are URL filter configuration settings in *UTM Profiles > Web Filter > URL Filter*.



URL blocking does not block access to other services that users can access with a web browser. For example, URL blocking does not block access to <ftp://ftp.example.com>. Instead, use firewall policies to deny FTP connections.

URL Filter page	
Lists each URL filter that you created. On this page, you can edit, delete or create a new URL filter.	
Create New	Creates a new URL filter list. When you select <i>Create New</i> , you are automatically redirected to the New List page. This page provides a name field and comment field. You must enter a name to go to the URL Filter Settings page.
Edit	Modifies settings within a URL filter list. When you select <i>Edit</i> , you are automatically redirected to the URL Filter Settings page.
Delete	<p>Removes the URL filter list from the list on the URL Filter page. The <i>Delete</i> icon is only available if the URL filter list is not selected in any profiles.</p> <p>To remove multiple URL filter list from within the list, on the URL Filter page, in each of the rows of the file filter lists you want removed, select the check box and then select <i>Delete</i>.</p> <p>To remove all URL filter list from the list, on the URL Filter page, select the check box in the check box column and then select <i>Delete</i>.</p>
Name	The available URL filter lists.
# Entries	The number of URL patterns in each URL filter list.
MMS Profiles (FortiOS Carrier only)	The name of the MMS profile
Comments	Optional description of each URL filter list.
Ref.	<p>Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a firewall policy; on the Profile page (<i>UTM Profiles > Antivirus > Profile</i>), 1 appears in <i>Ref.</i></p> <p>To view the location of the referenced object, select the number in <i>Ref.</i>, and the Object Usage window appears displaying the various locations of the referenced object.</p> <p>To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:</p> <ul style="list-style-type: none"> • View the list page for these objects – automatically redirects you to the list page where the object is referenced at. • Edit this object – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • View the details for this object – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy, and that firewall policy's settings appear within the table.
URL Filter Settings page	
Provides settings for configuring URLs that make up the URL filter, and also lists the URLs that you created. You are automatically redirected to this page from the New List Page. If you are editing a URL filter, you are automatically redirected to this page.	

Name	If you are editing an existing URL filter setting and want to change the name, enter a new name in this field. You must select <i>OK</i> to save the change.
Comments	If you are editing an existing URL filter setting and want to change or add a description, enter the new text in this field. You must select <i>OK</i> to save these changes.
Create New	Adds a URL address and filter settings to the list. When you select <i>Create New</i> , you are automatically redirected to the New URL Filter list.
Edit	Modifies the settings within a URL filter.
Delete	Removes an entry from the list. To remove multiple URL filters from within the list, on the URL Filter Settings page, in each of the rows of the filters you want removed, select the check box and then select <i>Delete</i> . To remove all URL filters from the list, on the URL Filter Settings page, select the check box in the check box column and then select <i>Delete</i> .
Enable	Enables a filter in the list.
Disable	Disables a filter in the list.
Move To	Moves the URL to any position in the list. When you select <i>Move To</i> , the Move URL Filter window appears. To move a URL, select the new position <i>Before</i> or <i>After</i> , which will place the current URL entry before or after the entry you enter in the (<i>URL</i>) field. For example, 1example.com is being moved after 3example.com, so 3example.com is entered in the (<i>URL</i>) field.
Remove All Entries	Removes all filter entries within the list on the URL Filter Settings page.
Enable	Indicates whether the URL is enable or disabled. A green check mark indicates that the URL is enabled; a gray check mark indicates that the URL is disabled.
URL	The URL address.
Action	The type of action the unit will take when there is a match.
Type	The type of URL. For example, the type of URL is <i>Regex</i> .
New URL Filter page Provides settings for configuring a URL to add to the filter list.	
URL	Enter the URL. Do not include http://. For details about URL formats, see “URL formats” on page 156 .
Type	Select a type from the drop-down list: <i>Simple</i> , <i>Regex</i> (regular expression), or <i>Wildcard</i> .

Action	<p>Select an action the unit will take.</p> <ul style="list-style-type: none"> • <i>Allow</i> – any attempt to access a URL that matches a URL pattern with an allow action is permitted. • <i>Exempt</i> – similar to <i>Pass</i> in that it allows trusted traffic to bypass the antivirus proxy operations, but it functions slightly differently; ensure you are aware of the network topology involving URLs that you applied the Exemption action. Additional information about the Exempt action is found in the UTM chapter of the FortiOS Handbook. • <i>Block</i> – attempts to access any URLs matching the URL pattern are denied; user is presented with a replacement message. • <i>Pass</i> – traffic to, and replay traffic from sites that match a URL pattern with a pass action will bypass all antivirus proxy operations, including FortiGuard Web Filter, web content filter, web script filters, and antivirus scanning. Make sure you trust the content of any site you pass, otherwise there may be a security risk.
Enable	Select to enable the URL. By default, the URL is enabled.



Type a top-level domain suffix (for example, “com” without the leading period) to block access to all URLs with this suffix.

URL formats

When adding a URL to the URL filter list, follow these rules:

How URL formats are detected when using HTTPS

If your unit does not support SSL content scanning and inspection or if you have selected the *URL filtering* option in web content profile for *HTTPS content filtering mode* under *Protocol Recognition*, filter HTTPS traffic by entering a top level domain name, for example, `www.example.com`. HTTPS URL filtering of encrypted sessions works by extracting the CN from the server certificate during the SSL negotiation. Since the CN only contains the domain name of the site being accessed, web filtering of encrypted HTTPS sessions can only filter by domain names.

If your unit supports SSL content scanning and inspection and if you have selected Deep Scan, you can filter HTTPS traffic in the same way as HTTP traffic.

How URL formats are detected when using HTTP

URLs with an action set to exempt are not scanned for viruses. If users on the network download files through the unit from trusted web site, add the URL of this web site to the URL filter list with an action set to exempt so the unit does not virus scan files downloaded from this URL.

- Type a top-level URL or IP address to control access to all pages on a web site. For example, `www.example.com` or `192.168.144.155` controls access to all pages at this web site.
- Enter a top-level URL followed by the path and filename to control access to a single page on a web site. For example, `www.example.com/news.html` or `192.168.144.155/news.html` controls the news page on this web site.

- To control access to all pages with a URL that ends with `example.com`, add `example.com` to the filter list. For example, adding `example.com` controls access to `www.example.com`, `mail.example.com`, `www.finance.example.com`, and so on.
- Control access to all URLs that match patterns created using text and regular expressions (or wildcard characters). For example, `example.*` matches `example.com`, `example.org`, `example.net` and so on.

Fortinet URL filtering supports standard regular expressions.



If virtual domains are enabled on the unit, web filtering features are configured globally. To access these features, select *Global Configuration* on the main menu.

Local Ratings

You can configure user-defined categories and then specify the URLs that belong to the category. This allows users to block groups of web sites on a per profile basis. The ratings are included in the global URL list with associated categories and compared in the same way the URL block list is processed.

Local ratings configuration settings

The following are local ratings configuration settings in *UTM Profiles > Web Filter > Local Ratings*.

Local Ratings page Lists each individual local rating that you created. On this page, you can edit, delete or create a new local rating. You can also disable or enable a local rating, as well as remove all local ratings from the page.	
Create New	Creates a new local rating. When you select <i>Create New</i> , you are automatically redirected to the New Local Rating page.
Edit	Modifies settings within a local rating. When you select <i>Edit</i> , you are automatically redirected to the Edit Local Rating page.
Delete	Select to remove a local rating from the list.
Enable	Enables a local rating within the list on the Local Ratings page.
Disable	Disables a local rating within the list on the Local Ratings page.
Remove All Entries	Removes all local ratings within the list on the Local Ratings page.
Search	Enter a word or name to search for the local rating within the list. Select <i>Go</i> to start the search.
#	The number identifying the order of the item in the list.
Enable	A green checkmark appears if the local rating is enabled. A gray x appears if the local rating is disabled.
URL	The URL address of the local rating.
Category	The category that was selected for the local rating.
Page controls	Use to navigate through the list of local ratings.

New Local Rating page

Provides settings for configuring the URL address that belongs to a category and classification rating. When editing a local rating, you are automatically redirected to the Edit Local Rating page which contains the same settings.

URL	Enter the URL address.
Category Rating	Select the ratings for the URL.



FortiGuard Web Filter

This section describes FortiGuard Web Filter for HTTP and HTTPS traffic.

FortiGuard Web Filter is a managed web filtering solution available by subscription from Fortinet. FortiGuard Web Filter enhances the web filtering features supplied with your FortiGate unit by sorting billions of web pages into a wide range of categories users can allow or block. The FortiGate unit accesses the nearest FortiGuard Web Filter Service Point to determine the category of a requested web page, and then applies the security policy configured for that user or interface.

FortiGuard Web Filter includes over 45 million individual ratings of web sites that apply to more than two billion pages. Pages are sorted and rated into several dozen categories administrators can allow or block. Categories may be added or updated as the Internet evolves. To make configuration simpler, you can also choose to allow or block entire groups of categories. Blocked pages are replaced with a message indicating that the page is not accessible according to the Internet usage policy.

FortiGuard Web Filter ratings are performed by a combination of proprietary methods including text analysis, exploitation of the web structure, and human raters. Users can notify the FortiGuard Web Filter Service Points if they feel a web page is not categorized correctly, so that the service can update the categories in a timely fashion.

The following topics are discussed in this section:

- [Before you begin](#)
- [FortiGuard Web Filter and your FortiGate unit](#)
- [Enable FortiGuard Web Filter](#)
- [Advanced FortiGuard Web Filter configuration](#)
- [Add or change FortiGuard Web Filter ratings](#)
- [Create FortiGuard Web Filter overrides](#)
- [Customize categories and ratings](#)
- [FortiGuard Web Filter examples](#)

Before you begin

Before you follow the instructions in this section, you should have a FortiGuard Web Filter subscription and your FortiGate unit should be properly configured to communicate with the FortiGuard servers. For more information about FortiGuard services, see the [FortiGuard Center](#) web page. You should also have a look at [“Web filter concepts”](#) on [page 133](#).

FortiGuard Web Filter and your FortiGate unit

When FortiGuard Web Filter is enabled in a web filter profile, the setting is applied to all firewall policies that use this profile. When a request for a web page appears in traffic controlled by one of these firewall policies, the URL is sent to the nearest FortiGuard server. The URL category is returned. If the category is blocked, the FortiGate unit provides a replacement message in place of the requested page. If the category is not blocked, the page request is sent to the requested URL as normal.

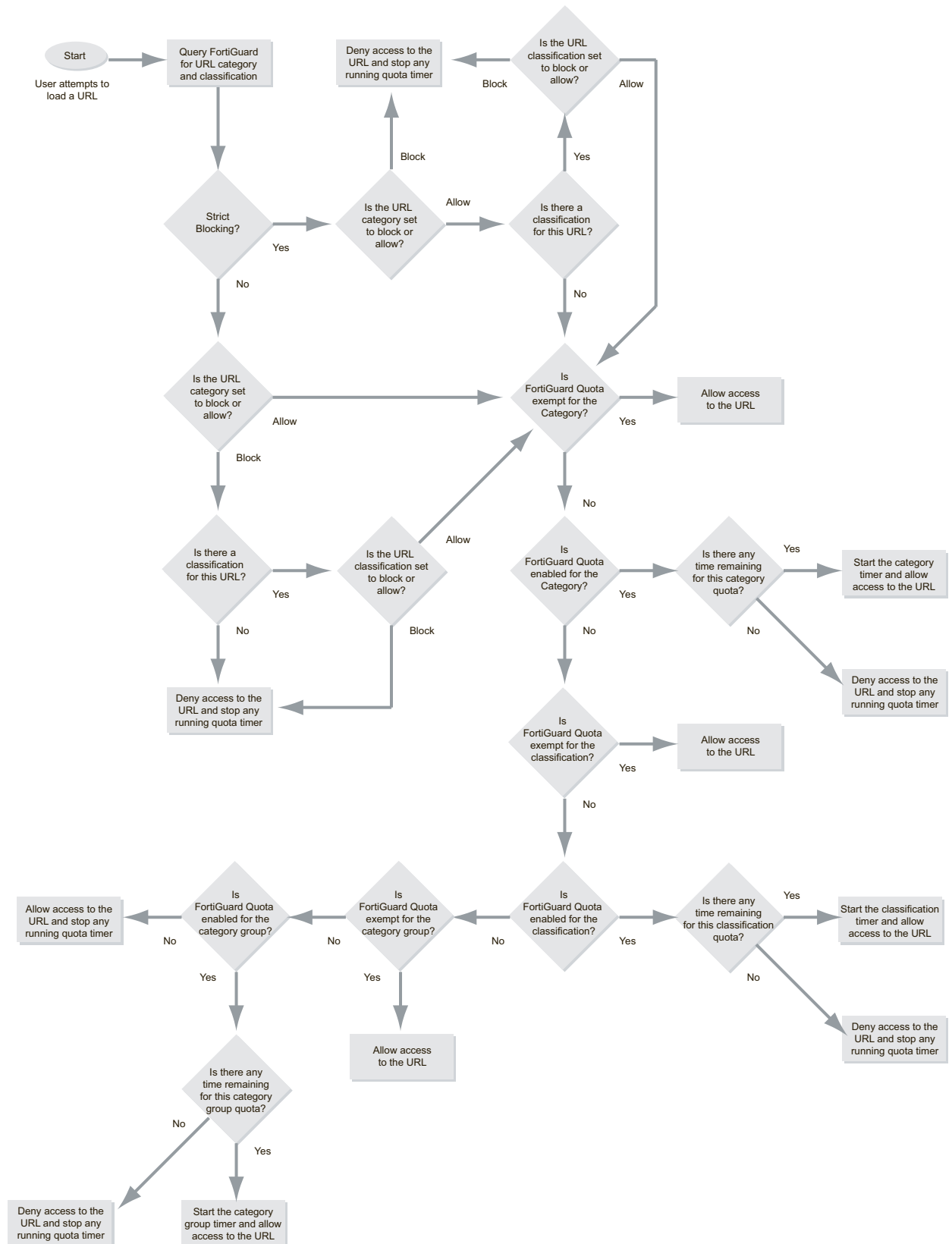
Order of web filtering

The FortiGate unit applies web filters in a specific order:

- 1 URL filter
- 2 FortiGuard Web Filter
- 3 web content filter
- 4 web script filter
- 5 antivirus scanning.

The flowchart in [Figure 9 on page 161](#) shows the steps involved in FortiGuard Web Filtering. Most features are included but some of the advanced options, including overrides, are not. The features appearing in the flowchart are described in this section.

Figure 9: FortiGuard Web Filter sequence of events



Enable FortiGuard Web Filter

FortiGuard Web Filter is enabled and configured within web filter profiles. Overrides, local categories, and local ratings are configured in *UTM Profiles > Web Filter*.

General configuration steps

- 1 Go to *UTM Profiles > Web Filter > Profile*.
- 2 Select the *Edit* icon of the web filter profile in which you want to enable FortiGuard Web Filter, or select *Create New* to add a new web filter profile.
- 3 Create a category filter in the profile.
- 4 The categories allow you to block or allow access to general or more specific web site categories. Configure access as required.
- 5 Save the filter and web filter profile.
- 6 To complete the configuration, you need to select the security policy controlling the network traffic you want to restrict. Then, in the security policy, enable *UTM* and select *Enable Web Filter* and select the appropriate web filter profile from the list.

Configuring FortiGuard Web Filter settings

FortiGuard Web Filter includes a number of settings that allow you to determine various aspects of the filtering behavior.

To configure FortiGuard Web Filter settings

- 1 Go to *UTM Profiles > Web Filter > Profile*.
- 2 Select the web filter profile in which you want to enable FortiGuard Web Filter from the drop down list in the Edit Web Filter Profile window title bar, or select *Create New* to add a new web filter profile.
- 3 The category groups are listed in a table. You can expand each category group to view and configure every category within the groups. If you change the setting of a category group, all categories within the group inherit the change.
- 4 Select the category groups and categories to which you want to apply an action.
- 5 Select an action from the *Change Action for Selected Categories* drop-down list immediately below the category table. Five actions are available:
 - *Allow* permits access to the sites within the category.
 - *Monitor* permits and logs access to sites in the category. You may also enable user quotas when enabling the monitor action.
 - *Warning* presents the user with a message, allowing them to continue if they choose.
 - *Authenticate* requires a user authenticate with the FortiGate unit before being allowed access to the category or category group.
 - *Block* prevents access to sites within the category. Users attempting to access a blocked site will receive a replacement message explaining that access to the site is blocked.
- 6 Select *OK*.

Configuring FortiGuard Web Filter usage quotas

In addition to using category and classification blocks and overrides to limit user access to URLs, you can set a daily timed access quota by category, category group, or classification. Quotas allow access for a specified length of time, calculated separately for each user. Quotas are reset every day at midnight.

Users must authenticate with the FortiGate unit. The quota is applied to each user individually so the FortiGate must be able to identify each user. One way to do this is to configure a security policy using the identity based policy feature. Apply the web filter profile in which you have configured FortiGuard Web Filter and FortiGuard Web Filter quotas to such a security policy.



The use of FortiGuard Web Filter quotas requires that users authenticate to gain web access. The quotas are ignored if applied to a security policy in which user authentication is not required.

When a user first attempts to access a URL, they're prompted to authenticate with the FortiGate unit. When they provide their username and password, the FortiGate unit recognizes them, determines their quota allowances, and monitors their web use. The category and classification of each page they visit is checked and FortiGate unit adjusts the user's remaining available quota for the category or classification.



Editing the web filter profile resets the quota timers for all users.

The quotas can be used with the user identities in a few ways. We have provided a couple of options as examples. One in which the use of the identity credentials is transparent to the user on one in which it is more obvious because the user is asked to authenticate.

To configure the FortiGuard Web Filter with quotas and without manual authentication.

- 1 Go to *UTM Profiles > Web Filter > Profile*.
- 2 Select the web filter profile in which you want to enable FortiGuard Web Filter from the drop down list in the Edit Web Filter Profile window title bar, or select *Create New* to add a new web filter profile.
- 3 Once in the profile editing window make sure that the profile has a name and that the Inspection Mode is set to Proxy (Quotas are not enabled in the *Flow-based* inspection Mode).
- 4 Select the required category groups. You may also expand the category groups to select individual categories.
- 5 Select the *Monitor* action.
- 6 Expand the *Quota on categories with Monitor, Warning and Authenticate Actions* line to activate the quota for the selected categories and category groups.
- 7 In the Quota section select *Create New*, select all of the categories that have the same quota time frame.
- 8 Select *Hours, Minutes, or Seconds* and enter the number of hours, minutes, or seconds. This is the daily quota allowance for each user.
- 9 Select *OK*.

10 Repeat steps 7 through 9 until all of the appropriate categories have been assigned a quota.

11 Select *Apply*.

To configure the FortiGuard Web Filter with quotas and with manual authentication.

- The only difference in the configuration between the 2 profiles is that in Step 5) you would select *Authenticate* as the action for the selected categories.

For both types of Web Filter profiles the next step would be to associate the profile with a firewall policy that has *Identity Based Policy* enabled. All of the users subject to the policy will be restricted by the quota whether or not they have to manually authenticate to access the Internet.

Quota hierarchy

You can apply quotas to categories and category groups. Only one quota per user can be active at any one time. The one used depends on how you configure the FortiGuard Web Filter.

When a user visits a URL, the FortiGate unit queries the FortiGuard servers for the category of the URL. From highest to lowest, the relative priority of the quotas are:

- 1 Category
- 2 Category group

So for example, the *General Interest - Business* category group contains the *Information and Computer Security* category. When a user visits a page in the *Information and Computer Security* category, the FortiGate unit will check for quotas in sequence:

- Is there is a quota set for the *Information and Computer Security* category? If there is, the category quota timer is started and the user is allowed access to the URL. If no time remains in the category quota, the URL is blocked and the user cannot access it for the remainder of the day.
- If no quota is set for the category, is there a quota set for the *General Interest - Business* category group? If there is, the category group quota timer is started and the user is allowed access to the URL. If no time remains in the category group quota, the URL is blocked and the user cannot access it for the remainder of the day.
- If there is no category group quota, the user is allowed to access the URL. Getting to this point means there are no quotas set for the page. The FortiGate unit will stop any running quota timer because the current URL has no quota.

Only one quota timer can be running at any one time for a single user. Whenever a quota timer is started or a page is blocked, the timer running because of the previous URL access, is stopped. Similarly, a URL with no quotas will stop a quota timer still running because of the URL the user previously accessed.

Quota exempt

The quota checking sequence occurs for every URL the user accesses. This is true for every web page, and every element of the web page that is loaded. For example, if a user loads a web page, the quota is checked for the web page as soon as it is loaded. If there is a photo on the page, it is also checked and the quota is adjusted accordingly.

This can cause unexpected behavior. For example, if the web page a user loads is in the *Information and Computer Security* category and it has a quota, the quota timer is started. The web page includes a number of graphics, so as these are loaded, each is checked and the appropriate quota is started. If they all share the same category rating, which they often will, there is no problem. However, if the last graphic or page element loaded comes from another site, the quota may not work as you expect. If the last

graphic is an ad, loaded from a site categorized as *Advertising*, the *Information and Computer Security* category quota timer will stop almost as soon as it is started because the FortiGate unit sees the ad URL and finds that it belongs to the *Advertising* category. If *Advertising* has a quota, its timer will start. If it is blocked or allowed, the *Information and Computer Security* category quota timer is stopped and the user can view the page without using the quota set to limit the *Information and Computer Security* category.

To solve this problem, you can configure a categories and category groups as exempt. This effectively allows the quota system to ignore it entirely. Any quota timer running when an exempt URL is encountered continues to run. An exempt category or category group, or classification can not have a quota. This may sound the same as simply disabling the quota and setting the FortiGuard Web Filter action to allow, but there is a difference. This difference is that the allow and block actions stop an already running quota timer, while the exempt action does not.

The exempt action is generally used for commonly accessed web pages that load elements from other sites that have different category ratings. Pages that load ads from advertising sites are the most common example.

To set a category or category group, see the [CLI Reference](#) for the `exempt-quota webfilter` command.

Checking quota usage

With quotas enabled, the FortiGate unit keeps track of quota usage for each user in each web filter profile. You can check the amount of quota usage for each user and their remaining time for each individual quota on the FortiGuard Quota page.

To view FortiGuard Web Filter quota usage

- 1 Go to *UTM Profiles > Monitor > FortiGuard Quota*.
- 2 The table shows the users who have used some or all of their quota allowance. The total time used is listed by web filter profile for each user.
- 3 Select the *View* icon in any row to view the remaining quota for each category, category group, and classification. A category, category group, or classification displayed in bold type indicates the quota currently in use.

Quotas are reset every day at midnight.

Advanced FortiGuard Web Filter configuration

The *Advanced Filter* section of the web filter profile provides a number of advanced filter options. The web filter options in the advance filter section unrelated to FortiGuard Web Filter are detailed in the web filter section, in [“Advanced web filter configuration” on page 142](#).

Provide Details for Blocked HTTP 4xx and 5xx Errors

Enable to have the FortiGate unit display its own replacement message for 400 and 500-series HTTP errors. If the server error is allowed through, malicious or objectionable sites can use these common error pages to circumvent web filtering.

Rate Images by URL (blocked images will be replaced with blanks)

Enable to have the FortiGate retrieve ratings for individual images in addition to web sites. Images in a blocked category are not displayed even if they are part of a site in an allowed category.

Blocked images are replaced on the originating web pages with blank place-holders. Rated image file types include GIF, JPEG, PNG, BMP, and TIFF.

Allow Websites When a Rating Error Occurs

Enable to allow access to web pages that return a rating error from the FortiGuard Web Filter service.

If your FortiGate unit cannot contact the FortiGuard service temporarily, this setting determines what access the FortiGate unit allows until contact is re-established. If enabled, users will have full unfiltered access to all web sites. If disabled, users will not be allowed access to any web sites.

Strict Blocking

This setting determines when the FortiGate unit blocks a site. Enable strict blocking to deny access to a site if any category or classification assigned to the site is set to *Block*. Disable strict blocking to deny access to a site only if all categories and classifications assigned to the site are set to *Block*.

All rated URLs are assigned one or more categories. URLs may also be assigned a classification. If *Rate URLs by domain and IP address* is enabled, the site URL and IP address each carry separately assigned categories and classifications. Depending on the FortiGuard rating and the FortiGate configuration, a site could be assigned to at least two categories and up to two classifications.

Rate URLs by Domain and IP Address

Enable to have the FortiGate unit request the rating of the site by URL and IP address separately, providing additional security against attempts to bypass the FortiGuard Web Filter.



FortiGuard Web Filter ratings for IP addresses are not updated as quickly as ratings for URLs. This can sometimes cause the FortiGate unit to allow access to sites that should be blocked, or to block sites that should be allowed.

If the rating determined by the domain name and the rating determined by the IP address defer the Action that is enforced will be determined by a weighting assigned to the different categories. The higher weighted category will take precedence in determining the action. This will have the side effect that sometimes the Action will be determined by the classification based on the domain name and other times it will be determined by the classification that is based on the IP address.

An example of how this would work would be if a URL's rating based on the domain name indicated that it belonged in the category *Lingerie and Swimsuit*, which is allowed but the category assigned to the IP address was *Pornography* which has an action of *Block*, because the *Pornography* category has a higher weight the effective action is *Block*.

Block HTTP Redirects by Rating

Enable to block HTTP redirects.

Many web sites use HTTP redirects legitimately but in some cases, redirects may be designed specifically to circumvent web filtering, as the initial web page could have a different rating than the destination web page of the redirect.

This option is not supported for HTTPS.

Daily log of remaining quota

Enable to log daily quota use.

As part of the quota reset at midnight, the FortiGate unit will record a log entry for every quota each user consumed during the day. These log entries are labeled with the sub-type `ftgd_quota`. Each entry includes the VDOM, user name, web filter profile name, category description, quota used (in seconds), and quota (in seconds). You can use log filtering to quickly limit the displayed entries to those you want, and generate reports from the logs.

Add or change FortiGuard Web Filter ratings

The FortiGuard Center web site allows you to check the current category assigned to any URL.

To check the category assigned to a URL

- 1 Using your web browser, go to the FortiGuard Center Web Filter URL Lookup & Submission page at <http://www.fortiguard.com/webfiltering/webfiltering.html>.
- 2 Enter the URL as directed.
- 3 Select *Search*.
- 4 If the URL has been rated by the FortiGuard web filter team, the category is displayed.

If a URL has not been rated, or you believe it is incorrectly rated, you can suggest the appropriate category and classification.

To add or change the category for a URL

- 1 Check the category assigned to the URL as described in the previous procedure.
- 2 Below the rating, select *Check to submit the URL*.
- 3 Enter your name, company, and email address.
- 4 Optionally, you may enter a comment.
- 5 Select the most appropriate category and classification for the URL.
- 6 Select *Submit* to send your submission to the FortiGuard web filter team.

Create FortiGuard Web Filter overrides

You can configure FortiGuard Web Filter to allow or deny access to web sites by category and classification. You may want to block a category but allow your users temporary access to one site within the blocked category. You may need to allow only some users to temporarily access one site within a blocked category. Do these things by using administrative and user overrides.

Understanding administrative and user overrides

The administrative overrides are backed up with the main configuration. The administrative overrides are not deleted when they expire and you can reuse them by extending their expiry dates. You can create administrative overrides either through the CLI or the web-based manager.

The user overrides are not backed up as part of the main configuration. These overrides are automatically deleted when they expire. You can only view and delete the user override entries. Users create user overrides using the authentication form opened from the block page when they attempt to access a blocked site, if override is enabled.

Customize categories and ratings

The FortiGuard Web Filter rating categories are general enough that virtually any web site can be accurately categorized in one of them. However, the rigid structure of the categories can create complications. For example, your company uses a web-based email provider. If you select the Web-based Email category, all sites categorized as web-based email providers, including the one your company uses, are blocked.

Local categories and local ratings allow you to assign sites to any category you choose. You can even create new categories. These settings apply only to your FortiGate unit. The changes you make are not sent to the FortiGuard Web Filter Service.

Creating local categories

Categories are labels that describe web site content. Creating your own category allows you to customize how the FortiGuard Web Filter service works.

Local categories appear in the web filter profile, under the FortiGuard Web Filter category list, in the *Local Categories* group. Local categories are empty when created. To populate local categories with web sites, see [“Customizing site ratings” on page 168](#).

To create a local category

```
config webfilter ftgd-local-cat
  edit "My local category"
end
```

The new local category is added to the list, but will remain empty until you add a web site to it.

Customizing site ratings

You may find it convenient to change the rating of a site. For example, if you want to block all the sites in a category except one, you can move the one site to a different category.

To customize a site rating

- 1 Go to *UTM Profiles > Web Filter > Local Ratings*.
- 2 Select *Create New*.
- 3 In the *URL* field, enter the URL of the site you want to change.
- 4 In the *Category Rating* table, select the category or categories to apply to the site.
If you created any local categories, a *Local Categories* group will appear.
- 5 Select *OK*.

FortiGuard Web Filter examples

FortiGuard Web Filter can provide more powerful filtering to your network because you can use it to restrict access to millions of sites by blocking the categories they belong to.

Configuring simple FortiGuard Web Filter protection

Small offices, whether they are small companies, home offices, or satellite offices, often have very simple needs. This example details how to enable FortiGuard Web Filter protection on a FortiGate unit located in a satellite office.

Creating a web filter profile

Most FortiGuard Web Filter settings are configured in a web filter profile. Web filter profiles are selected in firewall policies. This way, you can create multiple web filter profiles, and tailor them to the traffic controlled by the security policy in which they are selected. In this example, you will create one web filter profile.

To create a web filter profile — web-based manager

- 1 Go to *UTM Profiles > Web Filter > Profile*.
- 2 Select *Create New* in the Edit Web Filter Profile window title bar
- 3 In the *Name* field, enter `basic_FGWF`.
- 4 Select *OK*.
- 5 Select *Add Filter*.
- 6 Select a *Filter type* of *Category*.
- 7 the *FortiGuard Web Filtering* check boxes for the *HTTP* and *HTTPS* traffic types.
- 8 Select the *FortiGuard Web Filtering* expand arrow.
- 9 Select the *Potentially Liable*, *Controversial*, and *Security Risk* categories.
- 10 Select an *Action* of *Block*.
- 11 Select *OK*.
- 12 Enable *HTTPS Scanning*.
- 13 Select *Apply*.

Applying the web filter profile to a security policy

A web filter profile directs the FortiGate unit to scan network traffic only when it is selected in a security policy. When a web filter profile is selected in a security policy, its settings are applied to all the traffic the security policy handles.

To select the web filter profile in a security policy — web-based manager

- 1 Go to *Policy > Policy > Policy*.
- 2 Select a policy and choose the *Edit* icon.
- 3 Enable *UTM*.
- 4 Select the *Enable Web Filter* option.
- 5 Select the `basic_FGWF` profile from the list.
- 6 Select *OK* to save the security policy.

To select the web filter profile in a security policy — CLI

```
config firewall policy
  edit 1
    set utm-status enable
    set profile-protocol-options default
    set webfilter-profile basic_FGWF
  end
```

HTTP and HTTPS traffic handled by the security policy you modified will be monitored for attempts to access to the blocked sites. A small office may have only one security policy configured. If you have multiple policies, consider enabling web filter scanning for all outgoing policies.



If you have multiple policies, consider enabling web filter scanning for all outgoing policies.

School district

Continuing with the example in the Web filter section, you can use FortiGuard Web Filter to protect students from inappropriate material. For the first part of this example, see [“Web filtering example” on page 143](#).

To enable FortiGuard Web Filter

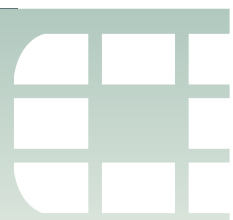
- 1 Go to *UTM Profiles > Web Filter > Profile*.
- 2 Select the web filter profile named *Students*.
- 3 Enable *HTTPS Scanning*.
- 4 Select *OK*.

The *Students* web filter profile has no FortiGuard Web Filtering filter. You must create and configure a filter to use FortiGuard Web Filter.

To configure the sites to block

- 1 Go to *UTM Profiles > Web Filter > Profile*.
- 2 Select the web filter profile named *Students*.
- 3 In the FortiGuard Categories table, select these categories: *Potentially Liable*, *Controversial*, and *Bandwidth Consuming*.
- 4 Select *Block* from the *Change Action for Selected Categories* to drop-down list.
- 5 Select *Apply* to save the web filter profile.

The students will not be able to access any of the web sites in those three general categories or the categories within them.



Data leak prevention

The FortiGate data leak prevention (DLP) system allows you to prevent sensitive data from leaving your network. When you define sensitive data patterns, data matching these patterns will be blocked, or logged and allowed, when passing through the FortiGate unit. You configure the DLP system by creating individual filters based on file type, file size, a regular expression, an advanced rule, or a compound rule, in a DLP sensor and assign the sensor to a security policy.

Although the primary use of the DLP feature is to stop sensitive data from leaving your network, it can also be used to prevent unwanted data from entering your network and to archive some or all of the content passing through the FortiGate unit.

This section describes how to configure the DLP settings.

The following topics are included:

- [Data leak prevention concepts](#)
- [Enable data leak prevention](#)
- [DLP document fingerprinting](#)
- [File filter](#)
- [Advanced rules](#)
- [Compound rules](#)
- [DLP archiving](#)
- [DLP examples](#)

Data leak prevention concepts

Data leak prevention examines network traffic for data patterns you specify. You define whatever patterns you want the FortiGate unit to look for in network traffic. The DLP feature is broken down into a number of parts.

DLP sensor

A DLP sensor is a package of filters. To use DLP, you must enable it in a security policy and select the DLP sensor to use. The traffic controlled by the security policy will be searched for the patterns defined in the filters contained in the DLP sensor. Matching traffic will be passed or blocked according to how you configured the filters.

DLP filter

Each DLP sensor has one or more filters configured within it. Filters can examine traffic for known files using DLP fingerprints, for files of a particular type or name, for files larger than a specified size, for data matching a specified regular expression, or for traffic matching an advanced rule or compound rule.

You can configure the action taken when a match is detected. The actions include Log Only, Block, Exempt, and Quarantine User, IP address, or Interface.

Logging is enabled by default, but you can also choose to archive matching traffic or generate an archive summary.

Fingerprint

Fingerprint scanning allows you to create a library of files for the FortiGate unit to examine. It will create checksum fingerprints so each file can be easily identified. Then, when files appear in network traffic, the FortiGate will generate a checksum fingerprint and compare it to those in the fingerprint database. A match triggers the configured action.

File filter

File filters use file filter lists to examine network traffic for files that match either file names or file types. For example, you can create a file filter list that will find files called secret.* and also all JPEG graphic files. You can create multiple file filter lists and use them in filters in multiple DLP sensors as required.

File size

This filter-type checks for files exceeding a configured size. All files larger than the specified size are subject to the configured action.

Regular expression

The FortiGate unit checks network traffic for the regular expression specified in a regular expression filter. Matching traffic is subject to the configured action.

Advanced rule

Each advanced rule includes a single condition and the type of traffic in which the condition is expected to appear. For more information about the supplied advanced rules, see [“Understanding the default advanced rules” on page 180](#).

Compound rule

Compound rules combine multiple advanced rules and require that all the conditions in the included advanced rules are true before the compound rule is triggered. For more information about the supplied compound rules, see [“Understanding the default compound rules” on page 181](#)

Enable data leak prevention

DLP examines your network traffic for data patterns you specify. You must configure DLP in sequence.

General configuration steps

Follow the configuration procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

- 1 Create a DLP sensor.

New DLP sensors are empty. You must create one or more filters in a sensor before it can examine network traffic.

- 2 Add one or more filters to the DLP sensor.

Each filter searches for a specific data pattern. When a pattern in the active DLP sensor appears in the traffic, the FortiGate unit takes the action configured in the matching filter.

- 3 Add the DLP sensor to one or more firewall policies that control the traffic to be examined.

Creating a DLP sensor

DLP sensors are collections of filters. You must also specify an action for the filter when you create it in a sensor. Once a DLP sensor is configured, you can select it a security policy profile. Any traffic handled by the security policy will be examined according to the DLP sensor configuration.

To create a DLP sensor

- 1 Go to *UTM Profiles > Data Leak Prevention > Sensor*.
- 2 Select the *Create New* icon on the Edit DLP Sensor window title bar.
- 3 In the *Name* field, enter the name of the new DLP sensor.
- 4 Optionally, you may also enter a comment. The comment appears in the DLP sensor list and can remind you of the details of the sensor.
- 5 Select the *Inspection Method*.

Proxy-based detection involves buffering the file or message and examining it as a whole. Advantages of proxy-based detection include a more thorough examination of attachments, especially archive formats and nesting.

Flow-based detection examines the file as it passes through the FortiGate unit without any buffering. Advantages of flow-based detection include speed and no interruption of detection during conserve mode.

- 6 Select *OK*.

The DLP sensor is created and the sensor configuration window appears.

- 7 Select *OK*.

A newly created sensor is empty, containing no filters. Without filters, the DLP sensor will do nothing.

Adding filters to a DLP sensor

Once you have created a DLP sensor, you need to add filters.

To add filters to a DLP sensor

- 1 Go to *UTM Profiles > Data Leak Prevention > Sensor*.
- 2 Select the Sensor in the Edit DLP Sensor window title bar drop-down list.
- 3 Select *Create New*.
- 4 Enter a filter name.

- 5 Select the type of filter from the *Filter By* drop-down list. The filter you choose determines the options available to you.

Fingerprint	<p>A fingerprint filter checks files in traffic against those in the FortiGate unit document fingerprint database. A match triggers the configured action.</p> <p>You must configure a document source or uploaded documents to the FortiGate unit for fingerprint scanning to work. For more information about document fingerprinting, see “DLP document fingerprinting” on page 176.</p>
File Type	Files in the network traffic are filtered by filename and file type.
File Pattern	<p>Select a file filter list that includes the file patterns and file types the network traffic will be examined for. Files matching the types or patterns in the selected list are treated according to the selected action.</p> <p>To create a file filter list, see “Creating a file filter list” on page 179.</p>
File Size	Files in the network traffic are filtered by size.
Maximum Size	Enter a file size in kilobytes. Files larger than the specified size are treated according to the selected action.
Regular Expression	Network traffic is examined for the pattern described by the regular expression.
Regular Expression	<p>Enter a regular expression. Traffic matching the regular expression is treated according to the selected action.</p> <p>For details about regular expression syntax, see “Using wildcards and Perl regular expressions” on page 281.</p>
Advanced Rule	Advanced rules detect a variety of data patterns in network traffic.
Advanced Rule	Select an advanced rule. Traffic matching the selected advanced rule is treated according to the selected action.
Compound Rule	Compound rules detect a variety of data patterns in network traffic. Compound rules are made of multiple advanced rules and all of the conditions must match for the compound rule to take effect.
Advanced Rule	Select a compound rule. Traffic matching the selected compound rule is treated according to the selected action.

- 6 Select the *Action* the FortiGate unit will take against network traffic matching the rule. A number of actions are available:

Log Only	The FortiGate unit will take no action on network traffic matching a rule with this action. The filter match is logged, however. Other matching filters in the same sensor may still operate on matching traffic.
Block	Traffic matching a filter with the block action will not be delivered. The matching message or download is replaced with the data leak prevention replacement message.
Quarantine User	<p>If the user is authenticated, this action blocks all traffic to or from the user using the protocol that triggered the rule and adds the user to the Banned User list.</p> <p>If the user is not authenticated, this action blocks all traffic of the protocol that triggered the rule from the user's IP address.</p> <p>If the banned user is using HTTP, FTP, or NNTP (or HTTPS if the FortiGate unit supports SSL content scanning and inspection) the FortiGate unit displays the "Banned by data leak prevention" replacement message for the protocol. If the user is using IM, the IM and P2P "Banned by data leak prevention" message replaces the banned IM message and this message is forwarded to the recipient. If the user is using IMAP, POP3, or SMTP (or IMAPS, POP3S, SMTPS if your FortiGate unit supports SSL content scanning and inspection) the Mail "Banned by data leak prevention" message replaces the banned email message and this message is forwarded to the recipient. These replacement messages also replace all subsequent communication attempts until the user is removed from the banned user list.</p>
Quarantine IP Address	This action blocks access for any IP address that sends traffic matching a filter with this action. The IP address is added to the Banned User list. The FortiGate unit displays the "NAC Quarantine DLP Message" replacement message for all connection attempts from this IP address until the IP address is removed from the banned user list.
Quarantine Interface	This action blocks access to the network for all users connecting to the interface that received traffic matching a filter with this action. The FortiGate unit displays the "NAC Quarantine DLP Message" replacement message for all connection attempts to the interface until the interface is removed from the banned user list.
Exempt	The exempt action prevents any filters from taking action on matching traffic. This action overrides the action assigned to any other matching filters.

Quarantine User, *Quarantine IP*, and *Quarantine Interface* provide functionality similar to NAC quarantine. However, these DLP actions block users and IP addresses at the application layer while NAC quarantine blocks IP addresses and interfaces at the network layer.



If you have configured DLP to block IP addresses and if the FortiGate unit receives sessions that have passed through a NAT device, all traffic from that NAT device — not just traffic from individual users — could be blocked. You can avoid this problem by implementing authentication.



To view or modify the replacement message text, go to *System > Config > Replacement Message*.

7 Select how traffic matching the rule will be archived.

Disable	Do not archive network traffic matching the rule.
Summary Only	Archive a summary of matching network traffic. For example, if applied to a rule governing email, the information archived includes the sender, recipient, message subject, message size, and other details.
Full	Archive the matching network traffic in addition to the summary information. For example, full archiving of email traffic includes the email messages and any attached files.



Archiving requires a FortiAnalyzer device or a subscription to the FortiGuard Analysis and Management Service.

8 Select *OK*.

The filter is added to the sensor. You may select *Create New* to add more filters, if required.

DLP document fingerprinting

One of the DLP techniques to detect sensitive data is fingerprinting (also called document fingerprinting). Most DLP techniques rely on you providing a characteristic of the file you want to detect, whether it's the file type, the file name, or part of the file contents. Fingerprinting is different in that you provide the file itself. The FortiGate unit then generates a checksum fingerprint and stores it. The FortiGate unit generates a fingerprint for all files detected in network traffic, and it is compared to all of the fingerprints stored in its fingerprint database. If a match is found, the configured action is taken.

The document fingerprint feature requires a FortiGate unit with internal storage. The document fingerprinting menu item does not appear on models without internal storage.

Any type of file can be detected by DLP fingerprinting and fingerprints can be saved for each revision of your files as they are updated.

To use fingerprinting you select the documents to be fingerprinted and then add fingerprinting filters to DLP sensors and add the sensors to firewall policies that accept the traffic to which to apply fingerprinting.

Fingerprinted Documents

The FortiGate unit must have access to the documents for which it generates fingerprints. One method is to manually upload documents to be fingerprinted directly to the FortiGate unit. The other is to allow the FortiGate unit to access a network share that contains the documents to be fingerprinted.

If only a few documents are to be fingerprinted, a manual upload may be the easiest solution. If many documents require fingerprinting, or if the fingerprinted documents are frequently revised, using a network share makes user access easier to manage.

To configure manual document fingerprints

- 1 Go to *UTM Profiles > Data Leak Prevention > Document Fingerprinting*.
- 2 In the Manual Document Fingerprints section, select *Create New*.
- 3 Select the file to be fingerprinted.
- 4 Choose a security level.
- 5 If the file is an archive containing other files, select *Process files inside archive* if you also want the individual files inside the archive to have fingerprints generated in addition to the archive itself.
- 6 Select *OK*.

The file is uploaded and a fingerprint generated.

To configure a fingerprint document source

- 1 Go to *UTM Profiles > Data Leak Prevention > Document Fingerprinting*.
- 2 In the Document Sources section, select *Create New*.
- 3 Configure the settings:

Name	Enter a descriptive name for the document source.
Server Address	Enter the IP address of the server.
User Name Password	Enter the user name and password of the account the FortiGate unit uses to access the server network share.
Path	Enter the path to the document folder.
Filename Pattern	You may enter a filename pattern to restrict fingerprinting to only those files that match the pattern. To fingerprint all files, enter an asterisk ("*").
Severity Level	Select a severity level. The severity is a tag for your reference that is included in the log files. It does not change how fingerprinting works.
Scan Periodically	To have the files on the document source scanned on a regular basis, select this option. This is useful if files are added or changed regularly. Once selected, you can choose Daily, Weekly, or Monthly update options, and enter the time of day the files are fingerprinted.
Advanced	Expand the Advanced heading for additional options.
Fingerprint files in subdirectories	By default, only the files in the specified path are fingerprinted. Files in subdirectories are ignored. Select this option to fingerprint files in subdirectories of the specified path.

Remove fingerprints for deleted files	Select this option to retain the fingerprints of files deleted from the document source. If this option is disabled, fingerprints for deleted files will be removed when the document source is rescanned.
Keep previous fingerprints for modified files	Select this option to retain the fingerprints of previous revisions of updated files. If this option is disabled, fingerprints for previous version of files will be deleted when a new fingerprint is generated.

4 Select OK.

File filter

File filter is a DLP option that allows you to block files based on their file name or their type.

- **File patterns** are a means of filtering based purely on the names of files. They may include wildcards (*). For example, blocking *.scr will stop all files with an scr file extension, which is commonly used for Windows screen saver files. Files trying to pass themselves off as Windows screen saver files by adopting the file-naming convention will also be stopped.

Files can specify the full or partial file name, the full or partial file extension, or any combination. File pattern entries are not case sensitive. For example, adding *.exe to the file pattern list also blocks any files ending with .EXE.

Files are compared to the enabled file patterns from top to bottom, in list order.

In addition to the built-in patterns, you can specify more file patterns to block. For details, see [“Creating a file filter list” on page 179](#).

- **File types** are a means of filtering based on an examination of the file contents, regardless of the file name. If you block the file type *Archive (zip)*, all zip archives are blocked even if they are renamed with a different file extension. The FortiGate examines the file contents to determine what type of file it is and then acts accordingly.

The FortiGate unit can take either of the following actions toward the files that match a configured file pattern or type:

- **Block:** the file is blocked and a replacement message is sent to the user. If both file pattern filtering and virus scan are enabled, the FortiGate unit blocks files that match the enabled file filter and does not scan these files for viruses.
- **Allow:** the file is allowed to pass.

The FortiGate unit also writes a message to the UTM log and sends an alert email message if configured to do so.



File filter does not detect files within archives. You can use file filter to block or allow the archives themselves, but not the contents of the archives.

General configuration steps

The following steps provide an overview of file filter configuration. For best results, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

- 1 Create a file filter list.

- 2 Create one or more file patterns or file types to populate the file filter list.
- 3 Enable the file filter list by adding it to a filter in a DLP sensor.
- 4 Select the DLP sensor in a security policy.

Creating a file filter list

Before your FortiGate unit can filter files by pattern or type, you must create a file filter list.

To create a file filter list

- 1 Go to *UTM Profiles > Data Leak Prevention > File Filter*.
- 2 Select *Create New*.
- 3 Enter a *Name* for the new file filter list.
- 4 Select *OK*.

The new list is created and the edit file filter list window appears. The new list is empty. You need to populate it with one or more file patterns or file types.

Creating a file pattern

A file pattern allows you to block or allow files based on the file name. File patterns are created within file filter lists.

To create a file pattern

- 1 Go to *UTM Profiles > Data Leak Prevention > File Filter*.
- 2 Select a file filter list.
- 3 Select the *Edit* icon.
- 4 Select *Create New*.
- 5 Select *File Name Pattern* as the *Filter Type*.
- 6 Enter the pattern in the *Pattern* field. The file pattern can be an exact file name or can include wildcards (*). The file pattern is limited to a maximum of 80 characters.
- 7 Select the action the FortiGate unit will take when it discovers a matching file: *Allow* or *Block*.
- 8 The filter is enabled by default. Clear the *Enable* check box if you want to disable the filter.
- 9 Select *OK*.

Creating a file type

A file type allows you to block or allow files based on the kind of file. File types are created within file filter lists.

To create a file type

- 1 Go to *UTM Profiles > Data Leak Prevention > File Filter*.
- 2 Select the *Edit* icon of the file filter list to which you will add the file type.
- 3 Select *Create New*.
- 4 Select *File Type* as the *Filter Type*.
- 5 Select the kind of file from the *File Type* list.

- 6 Select the action the FortiGate unit will take when it discovers a matching file: *Allow* or *Block*.
- 7 The filter is enabled by default. Clear the *Enable* check box if you want to disable the filter.
- 8 Select *OK*.

Advanced rules

A number of advanced rules are provided with your FortiGate unit. If you require additional rules, you can create your own.

Understanding the default advanced rules

You can use the default advanced rules as provided, or modify them to fit your needs.



These rules affect only unencrypted traffic types. If you are using a FortiGate unit that can decrypt and examine encrypted traffic, you can enable those traffic types in these rules to extend their functionality if required.



Before using the rules, examine them closely to ensure you understand how they will affect the traffic on your network.

All-Email, All-FTP, All-HTTP, All-IM, All-NNTP	These rules will detect all email, FTP, HTTP, instant messaging, and NNTP traffic.
Email-AmEx, Email-Canada-SIN, Email-US-SSN, Email-Visa-Mastercard	These four rules detect American Express numbers, Canadian Social Insurance Numbers, U.S. Social Security Numbers, or Visa and Mastercard numbers within the message bodies of SMTP, POP3, and IMAP email traffic.
HTTP-AmEx, HTTP-Canada-SIN, HTTP-US-SSN, HTTP-Visa-Mastercard	These four rules detect American Express numbers, Canadian Social Insurance Numbers, U.S. Social Security Numbers, or Visa and Mastercard numbers sent using the HTTP POST command. The HTTP POST command is used to send information to a web server. As written, these rules are designed to detect data the user is sending to web servers. This rule does not detect the data retrieved with the HTTP GET command, which is used to retrieve web pages.
Large-Attachment	This rule detects files larger than 5MB attached to SMTP, POP3, and IMAP email messages.
Large-FTP-Put	This rule detects files larger than 5MB sent using the FTP PUT command. Files received using FTP GET are not examined.

Large-HTTP-Post	This rule detects files larger than 5MB sent using the HTTP POST command. Files received using HTTP GET are not examined.
Email-Not-Webex, HTTP-Post-Not-Webex	These rules detect all traffic that is not generated by the WebEx web conference service. While not very useful on their own, these rules are used in the default compound rules.

Creating advanced rules

Most DLP functions can be accomplished using file filtering, file size, or regular expression features, but advanced rules do offer filtering features unavailable elsewhere in DLP. Creating your own advanced rules can be accomplished only using the CLI.

The general procedure when creating a DLP advanced rule is to specify the protocol, sub-protocol (if any), the field, and then the remaining options as required.

This example shows one way to create an advanced rule called email-confidential to detect the word “confidential” in the body of any email message. The rule can detect the word regardless of whether it is uppercase, lowercase, or a mixture of both.

To create a DLP advanced rule

```
config dlp rule
edit email-confidential
set protocol email
set sub-protocol imap pop3 smtp
set field body
set regexp /confidential/i
set description "Detect the word Confidential in email"
end
```

See the [CLI Reference](#) for a complete list of the DLP advanced rule commands and options.

Compound rules

A number of compound rules are provided with your FortiGate unit. If you require additional compound rules, you can create your own.

Understanding the default compound rules

You can use the default compound rules as provided, or modify them to fit your needs.



These rules affect only unencrypted traffic types. If you are using a FortiGate unit that can decrypt and examine encrypted traffic, you can enable those traffic types in these rules to extend their functionality if required.



Before using the rules, examine them closely to ensure you understand how they will affect the traffic on your network.

Email-SIN	This rule combines the Email-Canada-SIN and Email-Not-Webex advanced rules. If you use the Webex web conferencing service, the Email-Canada-SIN advanced rule can be mistakenly triggered by Webex traffic. Combining the advanced rules in a compound rules ensures that the Email-Canada-SIN rule will be triggered only by non-Webex network traffic.
HTTP-Post-SIN	This rule combines the HTTP-Canada-SIN and HTTP-Post-Not-Webex advanced rules. If you use the Webex web conferencing service, the HTTP-Canada-SIN advanced rule can be mistakenly triggered by Webex traffic. Combining the advanced rules in a compound rules ensures that the HTTP-Canada-SIN rule will be triggered only by non-Webex network traffic.

Creating compound rules

Compound rules are a very powerful feature to detect a specific set of circumstances. Because of this, you may need to create your own compound rules. Creating your own compound rules can be accomplished only using the CLI.

This example shows one way to create a compound rule called email-confidential-attachment to detect email messages that have the word “confidential” in the body of any email message and a file attachment of at least 5 MB in size.

To create a DLP compound rule

```
config dlp compound
edit email-confidential-attachment
set protocol email
set sub-protocol imap pop3 smtp
set member email-confidential
set member Large-Attachment
end
```

See the [CLI Reference](#) for a complete list of the DLP compound rule commands and options.

DLP archiving

DLP is typically used to prevent sensitive information from getting out of your company network, but it can also be used to record network use. This is called DLP archiving. The DLP engine examines email, FTP, IM, NNTP, and web traffic. Enabling archiving for rules when you add them to sensors directs the FortiGate unit to record all occurrences of these traffic types when they are detected by the sensor.

Since the archive setting is configured for each rule in a sensor, you can have a single sensor that archives only the things you want.

DLP archiving comes in two forms: *Summary Only*, and *Full*.

Summary archiving records information about the supported traffic types. For example, when an email message is detected, the sender, recipient, message subject, and total size are recorded. When a user accesses the Web, every URL the user visits recorded. The result is a summary of all activity the sensor detected.

For more detailed records, full archiving is necessary. When an email message is detected, the message itself, including any attachments, is archived. When a user accesses the Web, every page the user visits is archived. Far more detailed than a summary, full DLP archives require more storage space and processing.

Because both types of DLP archiving require additional resources, DLP archives are saved to a FortiAnalyzer unit or the FortiGuard Analysis and Management Service (subscription required).

Two sample DLP sensors are provided with DLP archiving capabilities enabled. If you select the `Content_Summary` sensor in a security policy, it will save a summary DLP archive of all traffic the security policy handles. Similarly, the `Content_Archive` sensor will save a full DLP archive of all traffic handled the security policy you apply it to. These two sensors are configured to detect all traffic of the supported types and archive them.

DLP examples

Blocking sensitive email messages

Someone in the Example.com corporation has been sending copies of the company president's monthly update email messages to the press. These messages have included the full header. Rather than try to block them, the IT department at Example.com will find out who is sending the messages using DLP.

All messages include the text `From: president@example.com` and `Subject: XYZ Monthly Update` where XYZ is the month the update applies to.

You will create a rule for the email address and a rule for the subject, combine them in a compound rule, and add the compound rule to a DLP sensor. You will then add the DLP sensor to the security policy that controls outgoing email traffic.

To create the "address" rule

```
config dlp rule
  edit "President address"
    set description "Finds president@example.com in email"
    set protocol email
    set sub-protocol imap pop3 smtp
    set field body
    set regexp-wildcard enable
    set regexp president@example.com
  end
```

To create the "subject" rule

```
config dlp rule
  edit "President subject"
    set description "Finds XYZ Monthly Update in email subject"
    set protocol email
    set sub-protocol imap pop3 smtp
    set field subject
    set regexp-wildcard enable
    set regexp "* Monthly Update"
  end
```

The asterisk (*) can represent any characters so the rule will match any monthly update.

Adding these two rules to a DLP sensor may generate a large number of false positives because any rule in a sensor will trigger the action. If the action were to log messages matching the address and subject rules in this example, then left as individual rules, the DLP sensor would log Monthly Updates from any employee and log all the president's email messages. In this case, you only want to know when both rules are true for a single message. To do this, you must first add the rules to a compound rule.

To create the “president + subject” compound rule.

```
config dlp compound
  edit "President + Subject"
    set protocol email
    set sub-protocol imap pop3 smtp
    set member "President address"
    set member "President subject"
  end
```

To create the “president” DLP sensor

- 1 Go to *UTM Profiles > Data Leak Prevention > Sensor*.
- 2 Select the *Create New* icon on the Edit DLP Sensor window title bar.
- 3 In the *Name* field, enter `president`.
- 4 In the *Comments* field, enter Finds “`president@example.com`” and “XYZ Monthly Update” in email.
- 5 Select *OK* to save the new sensor.
- 6 Select *Create New* to add a rule to the sensor.
- 7 Enter `President + Subject` for the *Filter Name*.
- 8 Set *Filter By* to *Compound Rule*.
- 9 Set *Advanced Rule* to *President + Subject*.
- 10 Set *Archive* to *Full*.
- 11 Select *OK*.

With the DLP sensor ready for use, you need to select it in the security policy.

To select the DLP sensor in the security policy

- 1 Go to *Policy > Policy > Policy*.
- 2 Select the security policy that controls outgoing email traffic.
- 3 Select the *Edit* icon.
- 4 Enable *UTM*.
- 5 Select the *Enable DLP Sensor* option.
- 6 Select the `president` sensor from the list.
- 7 Select *OK* to save the security policy.

With the DLP sensor specified in the correct security policy, any email message with both `president@example.com` and Monthly Update in the subject will trigger the sensor and the email message will be archived.

Data Leak Prevention interface reference

You can use the Data Leak Prevention (DLP) system to prevent sensitive data from leaving or entering your network. You can define sensitive data patterns, and data matching these patterns will be blocked and/or logged or archived when passing through the unit. The DLP system is configured by creating individual rules, combining the rules into DLP sensors, and then assigning a sensor to a firewall policy.

Although the primary use of the DLP feature is to stop sensitive data from leaving your network, it can also be used to prevent unwanted data from entering your network and to archive some or all of the content passing through the unit.

This topic includes the following:

- [Sensor](#)
- [Document Fingerprinting](#)
- [File Filter](#)
- [DLP archiving](#)

Sensor

DLP sensors are simply collections of DLP rules and DLP compound rules. The DLP sensor also includes settings such as action, archive, and severity for each rule or compound rule. Once a DLP sensor is configured, it can be specified in a firewall policy. Any traffic handled by the policy in which the DLP sensor is specified will enforce the DLP sensor configuration.

You can create a new DLP sensor and configure it to include the DLP rules and DLP compound rules required to protect the traffic leaving your network.

A DLP sensor must be created before it can be configured by adding rules and compound rules.



Before use, examine the sensors and rules in the sensors closely to ensure you understand how they will affect the traffic on your network.

DLP sensor configuration settings

The following are DLP sensor configuration settings in *UTM Profiles > Data Leak Prevention > Sensor*.

Sensor page Lists each individual DLP sensor that you created, as well as the default DLP sensors. On this page, you can edit DLP sensors (default or ones that you created), delete or create new DLP sensors. You are redirected to this page when you select <i>View List</i> on the Edit DLP Sensor page.	
Create New	Creates a new DLP sensor. When you select <i>Create New</i> , you are automatically redirected to the New DLP List page. This page provides a name field and comment field. You must enter a name to go to the Sensor Settings page.
Edit	Modifies settings within a DLP sensor. When you select <i>Edit</i> , you are automatically redirected to the Edit DLP Sensor page.
Delete	Removes a DLP sensor from the list. To remove multiple DLP sensors from within the list, on the Sensor page, in each of the rows of the sensors you want removed, select the check box and then select <i>Delete</i> . To remove all DLP sensors from the list, on the Sensor page, select the check box in the check box column and then select <i>Delete</i> .
Clone	Select to use an existing DLP sensor's settings as the basis for a new DLP sensor's settings.
Name	The DLP sensor name. There are six default sensors. The following default DLP sensors are provided with your unit. You can use these as provided, or modify them as required.
Comments	The optional description of the DLP sensor.

Ref.	<p>Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a firewall policy; on the Profile page (<i>UTM Profiles > Antivirus > Profile</i>), 1 appears in <i>Ref.</i></p> <p>To view the location of the referenced object, select the number in <i>Ref.</i>, and the Object Usage window appears displaying the various locations of the referenced object.</p> <p>To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:</p> <ul style="list-style-type: none"> • View the list page for these objects – automatically redirects you to the list page where the object is referenced at. • Edit this object – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • View the details for this object – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy, and that firewall policy's settings appear within the table.
Content_Archive (default)	<p>DLP archive all email (POP3, IMAP, and SMTP), FTP, HTTP, and IM traffic. For each rule in the sensor, <i>Archive</i> is set to <i>Full</i>. No blocking or quarantine is performed. See “DLP archiving” on page 196.</p> <p>You can add the <i>All-Session-Control</i> rule to also archive session control content.</p> <p>If you have a unit that supports SSL content scanning and inspection, you can edit the <i>All-Email</i> rule to archive POP3S, IMAPS, and SMTPS traffic. You can also edit the <i>All-HTTP</i> rule to archive HTTPS traffic.</p>
Content_Summary (default)	<p>DLP summary archive all email (POP3, IMAP, and SMTP), FTP, HTTP, and IM traffic. For each rule in the sensor, <i>Archive</i> is set to <i>Summary Only</i>. No blocking or quarantine is performed. See “DLP archiving” on page 196.</p> <p>You can add the <i>All-Session-Control</i> rule to also archive session control content.</p> <p>If you have a unit that supports SSL content scanning and inspection, you can edit the <i>All-Email</i> rule to archive POP3S, IMAPS, and SMTPS traffic.</p> <p>You can also edit the <i>All-HTTP</i> rule to archive HTTPS traffic.</p>

Credit-Card (default)	<p>The number formats used by American Express, Visa, and Mastercard credit cards are detected in HTTP and email traffic.</p> <p>As provided, the sensor is configured not to archive matching traffic and an action of <i>None</i> is set. Configure the action and archive options as required.</p>
Large-File (default)	<p>Files larger than 5MB will be detected if attached to email messages or if send using HTTP or FTP.</p> <p>As provided, the sensor is configured not to archive matching traffic and an action of <i>None</i> is set. Configure the action and archive options as required.</p>
SSN-Sensor (default)	<p>The number formats used by U.S. Social Security and Canadian Social Insurance numbers are detected in email and HTTP traffic.</p> <p>As provided, the sensor is configured not to archive matching traffic and an action of <i>None</i> is set. Configure the action and archive options as required.</p>
<p>Edit DLP Sensor page</p> <p>Provides settings for configuring rules that are added to DLP sensors. When you select <i>Create New</i> to create a new sensor, you are automatically redirected to the New DLP Sensor page. You must enter a name for the sensor in the <i>Name</i> field to continue configuring the sensor, at which time you are redirected to the Sensor Settings page. When you select <i>Create New</i> on this page, you are redirected to the New DLP Sensor Rule page.</p> <p>Note: Enabling logging or NAC quarantine is available in the CLI.</p>	
Name	If you are editing an existing sensor and want to change the name, enter a name in this field. You must select <i>OK</i> to save the change.
Comment	If you are editing an existing sensor and want to change or add a description, enter the new text in this field. You must select <i>OK</i> to save these changes.
Inspection Method	Select the type of DLP inspection method.
Flow-based Detection	Select to enable flow-based DLP scanning. Flow-based is a non-proxy solution which provides high concurrent session, high session rate, and low-latency DLP service.
Proxy-based Detection (Extended)	Select to enable a proxy-based detection scanning method.
Create New	<p>Adds a new rule or compound rule to the sensor. When you select a specific type of member, either <i>Compound rule</i> or <i>Rule</i>, different options become available.</p> <p>When you select <i>Create New</i>, you are automatically redirected to the New DLP Sensor Rule page.</p>
Edit	Modifies a rule or compound rule. When you select <i>Edit</i> , you are automatically redirected to Edit DLP Sensor Rule page.

Delete	<p>Removes a compound rule or a rule from the list.</p> <p>To remove multiple compound rules or rules from the list, on the DLP Sensor Settings page, in each of the rows of the compound rules or rules you want removed, select the check box and then select <i>Delete</i>.</p> <p>To remove all compound rules and/or rules from the list, select the check box in the check box column and then select <i>Delete</i>.</p>
Filter Name	The name of the rule that you have created. This is often referred to as a filter because it can filter the information using the rule applied.
Type	The type of rule that was applied, such as compound rule or fingerprint.
Action	<p>The action configured for each rule. If the selected action is <i>None</i>, no action will be listed.</p> <p>Although archiving is enabled independent of the action, the <i>Archive</i> designation appears with the selected action.</p> <p>For example, if you select the <i>Block</i> action and set <i>Archive</i> to <i>Full</i> for a rule, the action displayed in the sensor rule list is <i>Block, Archive</i>.</p>
Archive	The type of archiving that is selected for that rule. For example, summary only.
New DLP Sensor Filter page Provides settings for configuring filter, such as compound rule or document finger print.	
Filter Name	Enter a name for the rule.
Filter By	<p>Select what the DLP sensor will filter by, for example compound rule. You can choose to filter by the following rules:</p> <ul style="list-style-type: none"> • Finger Print • File Type • File Size • Regular Expression • Advanced Rule • Compound Rule
Sensitivity	The sensitivity level for document fingerprinting. Appears only when <i>Filter By</i> is <i>Finger Print</i> .
Advanced Rule	Select the advance rule that you want applied to the filter. Appears when <i>Filter By</i> is either <i>Compound Rule</i> or <i>Advanced Rule</i> .
Regular Expression	Enter the regular expression in the filed provided. Appears only when <i>Filter By</i> is <i>Regular Expression</i> .
Maximum Size	Enter the maximum file size in kB. Appears only when <i>Filter By</i> is <i>File Size</i> .

File Pattern	Select the type of file pattern. Appears only when <i>Filter By</i> is <i>File Type</i> .
Action	Select an action that the unit will take for that particular rule or compound rule.



DLP prevents duplicate action. Even if more than one rule in a sensor matches some content, DLP will not create more than one DLP archive entry, quarantine item, or ban entry from the same content.

Document Fingerprinting

DLP document fingerprinting allows you to better protect specific documents from leakage. Document fingerprinting, in this sense, is a method of uniquely identifying a document. This method breaks up files into chunks, taking a checksum of those chunks and using that checksum as the fingerprint. The fingerprint is then applied to a DLP filter rule within a DLP sensor which is then used during the scanning process of DLP activity.

Document Fingerprint page	
Lists the document sources as well as the document files that were manually inputted.	
Document Sources section	
Lists the configured document sources for document fingerprinting.	
Create New	Creates a new document source. When you select <i>Create New</i> , you are automatically redirected to the Document Source page.
Delete	Removes a document source from within the list. To remove multiple document sources from the list, in the Document Sources section of the page, in each of the rows of sources you want removed, select the check box and then select <i>Delete</i> . To remove all document sources from the list, select the check box in the check box column and then select <i>Delete</i> .
View	Select to view the document sources' information.
Name	The name of the document source.
Server	The source's IP address or server IP address of where the documents/files are located.
Path	The location of where the files are located on the server.
Sensitivity Level	The level of sensitivity for the documents on the server.
# Documents	The total number of documents for fingerprinting.
Manual Document Fingerprints section	
Lists each individual document or file that you uploaded to the FortiGate unit for fingerprinting.	
Create New	Uploads a file or document that you want for fingerprinting. When you select <i>Create New</i> , you are automatically redirected to the Upload File for Fingerprinting page. For more information about uploading individual documents for fingerprinting, see " Manual Document Fingerprints " on page 192.

Delete	Removes a document from within the list. To remove multiple documents from the list, in the Manual Document Fingerprints section of the page, in each of the rows of documents you want removed, select the check box and then select <i>Delete</i> . To remove all documents from the list, select the check box in the check box column and then select <i>Delete</i> .
Name	The name of the document.
Sensitivity Level	The level of sensitivity given to that uploaded document.

Document Sources configuration settings

The following are configuration settings for document sources in *UTM Profiles > Data Leak Prevention > Document Fingerprinting*.

Document Source page	
Provides settings for configuring the document sources, or servers, that contain the files or documents that you want to prevent being leaked from your intranet.	
Name	Enter the name of the document source.
Server Type	Select the type of server, such as a windows share server. The Windows Share server is the default server type available.
Server Address	Enter the server's IP address.
User Name	Enter the name of the user that logs in to the server.
Password	Enter the user's password that is required to log in to the server.
Path	Enter the location of where the files are located on the server.
Filename Pattern	Enter the pattern of the name of the files, such as *.pdf.
Sensitivity Level	Select the type of sensitivity level you created in the CLI, using the <code>config dlp fp-sensitivity</code> command. There are three default sensitivity levels: Private, Critical and Warning.
Scan Periodically	Select to schedule when the FortiGate unit scans the server. When you select the check box to enable this, the following options appear.
Daily	Select to schedule a daily scan. Enter the hour and minutes in the fields provided.
Weekly	Select to schedule a scan during a day of the week and at a specific time. When you select <i>Weekly</i> , <i>Weekday</i> appears. Select a day from the drop-down list in <i>Weekday</i> and then enter the hour and minutes in the fields provided. For example, a scan will occur every Monday at 5:30.

Monthly	Select the day of the month to scan. Enter the date of the month, such as 5, in the <i>Date</i> field. Enter the hour and minutes in the fields provided.
Advanced	Expand to enable or disable any of the following: <ul style="list-style-type: none"> • <i>Fingerprint files in subdirectories</i> – fingerprints files that are in subdirectories as well as in directories • <i>Remove fingerprints for deleted files</i> – removes fingerprints from files that are deleted from the source or server. • <i>Keep previous fingerprints for modified files</i> – keeps the fingerprints for files that were recently modified.

Manual Document Fingerprints

The Manual Document Fingerprints section of the DLP Fingerprint page allows you to upload a document that will be fingerprinted by the FortiGate unit.

The following are settings for uploading documents for fingerprinting in *UTM Profiles > Data Leak Prevention > Document Fingerprinting*.

Upload File for Fingerprinting page	
Uploads the individual files that you want to provide for fingerprinting.	
File	Enter the file name.
Sensitivity Level	Select the sensitivity level from the drop-down list.
Process files inside archives	Select to enable the FortiGate unit to process files that are inside archive files.

File Filter

The Filter menu allows you to configure filtering options that block specific file patterns and file types. Files are compared to the enabled file patterns and then the file types from top to bottom. If a file does not match any specified patterns or types, it is passed along to antivirus scanning (if enabled). In effect, files are passed if not explicitly blocked. The unit also writes a message to the virus log and sends an alert email message if configured to do so.

The unit can take either of these actions toward files that match a configured file pattern or type:

- Allow: the file is allowed to pass.
- Block: the file is blocked and a replacement messages will be sent to the user. If both file filter and virus scan are enabled, the unit blocks files that match the enabled file filter and does not scan these files for viruses.
- Intercept: the file will be archived to the local hard disk or the FortiAnalyzer unit. (FortiOS Carrier only)

By using the *Allow* action, this behavior can be reversed with all files being blocked unless explicitly passed. Simply enter all the file patterns or types to be passed with the allow attribute. At the end of the list, add an all-inclusive wildcard (*.*) with a block action. Allowed files continue to antivirus scanning (if enabled) while files not matching any allowed patterns are blocked by the wildcard at the end. For standard operation, you can choose to disable file filter in the profile, and enable it temporarily to block specific threats as they occur.

The unit is preconfigured with a default list of file patterns:

- executable files (*.bat, *.com, and *.exe)
- compressed or archive files (*.gz, *.rar, *.tar, *.tgz, and *.zip)
- dynamic link libraries (*.dll)
- HTML application (*.hta)
- Microsoft Office files (*.doc, *.ppt, *.xl?)
- Microsoft Works files (*.wps)
- Visual Basic files (*.vb?)
- screen saver files (*.scr)
- program information files (*.pif)
- control panel files (*.cpl)

The unit can detect the following file types:

Table 14: Supported file types

arj	activemime	aspack	base64	bat	binhex	bzip	bzip2
cab	class	cod	elf	exe	fsg	gzip	hlp
hta	html	jad	javascript	lzh	mime	msc	msoffice
petite	prc	rar	sis	tar	upx	uue	zip
unknown	ignored						



The “unknown” type is any file type that is not listed in the table. The “ignored” type is the traffic the unit typically does not scan. This includes primarily streaming audio and video.

File filter configuration

You can add multiple file filter lists to the antivirus profile. For file patterns, you can add a maximum of 5000 patterns to a list. For file types, you can select only from the supported types.

The following are file filter configuration settings in *UTM Profiles > Data Leak Prevention > File Filter*.

<i>File Filter page</i> Lists each individual file filter that you created. On this page, you can edit, delete or create a new file filter.	
Create New	Creates a new file filter. When you select <i>Create New</i> , you are automatically redirected first to the New List page. You must enter a name for the file filter list in the <i>Name</i> field on the New List page and then select <i>OK</i> then be redirected to the File Filter Settings page.
Delete	Removes the file filter list from the list on the File Filter page. To remove multiple file filter lists from within the list, on the File Filter page, in each of the rows of the file filter lists you want removed, select the check box and then select <i>Delete</i> . To remove all file filter lists from the list, on the File Filter page, select the check box in the check box column and then select <i>Delete</i> .
Edit	Modifies the settings within a file filter list. When you select <i>Edit</i> , you are redirected to the File Filter Settings page.
Name	The name of the file filter list.
# Entries	The number of file patterns or file types in each file filter list.
DLP Rule	The DLP rules in which each filter is used.
Comments	An optional description of each file filter list.
Ref.	Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a firewall policy; on the Profile page (<i>UTM Profiles > Antivirus > Profile</i>), 1 appears in <i>Ref.</i> . To view the location of the referenced object, select the number in <i>Ref.</i> , and the Object Usage window appears displaying the various locations of the referenced object. To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window: <ul style="list-style-type: none"> • View the list page for these objects – automatically redirects you to the list page where the object is referenced at. • Edit this object – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • View the details for this object – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy, and that firewall policy's settings appear within the table.
<i>File Filter Settings page</i> Provides settings for configuring multiple file patterns and file types that make up a file filter. This page also lists the file patterns and file types that were created for the file filter. If you are editing a file filter, you are redirected to this page.	

Name	The name that was entered in the <i>Name</i> field on the New List page. To change the name, edit the text in this field and select <i>OK</i> .
Comment	The comment that was entered in the <i>Comment</i> field on the New List page. If you want to edit or add the description, enter the text in this field and select <i>OK</i> .
Create New	Creates a new file filter pattern or type within the list on the File Filter Settings page. When you select <i>Create New</i> , you are automatically redirected to the New File Filter page.
Edit	Modifies settings within the file pattern/type and action. When you select <i>Edit</i> , you are automatically redirected to the Edit File Filter page.
Delete	Removes the file pattern or type from the list on the File Filter Settings page. To remove multiple file filter lists from within the list, on the File Filter page, in each of the rows of the file filter lists you want removed, select the check box and then select <i>Delete</i> . To remove all file filter lists from the list, on the File Filter page, select the check box in the check box column and then select <i>Delete</i> .
Enable	Enables a disabled file pattern or type.
Disable	Disables a file pattern or type.
Move To	Moves the file pattern or type to any position in the list. When you select <i>Move To</i> , the Move AV File Filter Entry window appears. To move a file pattern or type, select the new position <i>Before</i> or <i>After</i> , which will place the current entry before or after the entry you enter in (<i>Entry</i>). Enter the entry's name in the (<i>Entry</i>) field.
Filter	The current list of file patterns and types.
Action	Files matching the file patterns and types can be set to <i>Block</i> or <i>Allow</i> .
Enable	Indicates that the file pattern or file type is either enabled or disabled. A green check mark indicates that the pattern or type is enabled; a gray x indicates that it is disabled.
New File Filter page Provides settings for configuring the file pattern or file type for the list. When you select <i>Create New</i> on the File Filter Settings page, you are automatically redirected to this page.	
Filter Type	Select <i>File Name Pattern</i> or <i>File Type</i> .
File Type	Select a file type from the list. Appears only when <i>File Type</i> is selected in <i>Filter Type</i> .
Pattern	Enter the file pattern. The file pattern can be an exact file name or can include wildcards. The file pattern can be 80 characters long.
Action	Select an action from the drop down list: <i>Block</i> or <i>Allow</i> .
Enable	Select to enable or disable the filter.



The default file pattern list catalog is called *builtin-patterns*.

DLP archiving

You can use DLP archiving to collect and view historical logs that have been archived to a FortiAnalyzer unit or the FortiGuard Analysis and Management Service. DLP archiving is available for FortiAnalyzer when you add a FortiAnalyzer unit to the Fortinet configuration. The FortiGuard Analysis server becomes available when you subscribe to the FortiGuard Analysis and Management Service.

You can configure full DLP archiving and summary DLP archiving. Full DLP archiving includes all content, for example, full email DLP archiving includes complete email messages and attachments. Summary DLP archiving includes just the meta data about the content, for example, email message summary records include only the email header.

You can archive Email, FTP, HTTP, IM, and session control content:

- Email content includes IMAP, POP3, and SMTP sessions. Email content can also include email messages tagged as spam by Email filtering. If your unit supports SSL content scanning and inspection, Email content can also include IMAPS, POP3S, and SMTPS sessions.
- HTTP content includes HTTP sessions. If your unit supports SSL content scanning and inspection HTTP content can also include HTTPS sessions.
- IM content includes AIM, ICQ, MSN, and Yahoo! sessions.
- MMS content includes MM1, MM3, MM4, and MM7 sessions. (FortiOS Carrier only)
- Session control content includes SIP, SIMPLE and SCCP sessions. Only summary DLP archiving is available for SIP and SCCP. Full and summary DLP archiving is available for SIMPLE.

You add DLP sensors to archive Email, Web, FTP, IM, and session control content. Archiving of spam email messages is configured in the DLP sensor.

In FortiOS Carrier, MMS archiving is configured in MMS profiles.

DLP archiving is enabled in the DLP sensor itself. DLP sensors are located in *UTM Profiles > Data Leak Prevention > Sensor*. You can also use either Content_Archive or Content_Summary sensors to archive DLP logs instead of creating a new DLP sensor for archiving purposes.

You can now create a session control DLP rule that includes SIP, SIMPLE or SCCP for DLP archiving within the CLI.



Application control

Using the application control UTM feature, your FortiGate unit can detect and take action against network traffic depending on the application generating the traffic. Based on FortiGate Intrusion Protection protocol decoders, application control is a user-friendly and powerful way to use Intrusion Protection features to log and manage the behavior of application traffic passing through the FortiGate unit. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols.

The FortiGate unit can recognize the network traffic generated by a large number of applications. You can create application control sensors that specify the action to take with the traffic of the applications you need to manage and the network on which they are active, and then add application control sensors to the firewall policies that control the network traffic you need to monitor.

This section describes how to configure the application control settings.

If you enable virtual domains (VDOMs) on the Fortinet unit, you need to configure application control separately for each virtual domain.

The following topics are included in this section:

- [Application control concepts](#)
- [Enable application control](#)
- [Application traffic shaping](#)
- [Application control monitor](#)
- [Application control packet logging](#)
- [Application considerations](#)
- [Application control examples](#)

Application control concepts

You can control network traffic generally by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself in the security policy. If you want to control the flow of traffic from a specific application, these methods may not be sufficient to precisely define the traffic. To address this problem, the application control feature examines the traffic itself for signatures unique to the application generating it. Application control does not require knowledge of any server addresses or ports. The FortiGate unit includes signatures for over 1000 applications, services, and protocols.

Updated and new application signatures are delivered to your FortiGate unit as part of your FortiGuard Application Control Service subscription. Fortinet is constantly increasing the number of applications that application control can detect by adding applications to the [FortiGuard Application Control Database](#). Because intrusion protection protocol decoders are used for application control, the application control database is part of the [FortiGuard Intrusion Protection System Database](#) and both of these databases have the same version number.

To view the version of the application control database installed on your FortiGate unit, go to the *License Information* dashboard widget and find the *IPS Definitions* version.

To see the complete list of applications supported by FortiGuard Application Control go to the [FortiGuard Application Control List](#). This web page lists all of the supported applications. You can select any application name to see details about the application.

Enable application control

Application control examines your network traffic for traffic generated by the applications you want it to control.

General configuration steps

Follow the configuration procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

- 1 Create an application sensor.
- 2 Configure the sensor to include the signatures for the application traffic you want the FortiGate unit to detect. Configure each entry to allow or pass the traffic.
- 3 Enable UTM and application control in a security policy and select the application sensor.

Creating an application sensor

You need to create an application sensor before you can enable application control.

To create an application sensor

- 1 Go to *UTM Profiles > Application Control > Application Sensor*.
- 2 Select the *Create New* icon in the title bar of the *Edit Application Sensor* window.
- 3 In the *Name* field, enter the name of the new application sensor.
- 4 Optionally, you may also enter a comment.
- 5 Select *OK*.

The application sensor is created and the sensor configuration window appears. A newly created application sensor is empty. Without applications, the application sensor will have no effect.

Adding applications to an application sensor

Once you have created an application sensor, you need to need to define the applications that you want to control.

You can add applications using application entries and application filters. Entries allow you to choose individual applications. Filters allow you to choose application attributes and all the applications with matching attributes are included in the filter.



The sequence of the entries in the table is significant. The entries are checked against the traffic in sequence, from top to bottom. If a match is found and the action is *Block* or *Reset*, the action is performed and further checking is stopped. If the action is *Monitor* the traffic is checked against all of the signatures in the sensor and the best match to the signature is the one that is logged.

To add an application entry to an application sensor

- 1 Go to *UTM Profiles > Application Control > Application Sensor*.
- 2 Select an application sensor from the drop-down list in the *Edit Application Sensor* window title bar.

- 3 Select the *Create New* drop-down icon in the sensor and choose *Entry*.
- 4 Using the *Category* selection, choose the type of application you want to add. For example, if you want to add Facebook chat, choose *im*.

The *Category* selection displays only the options available in the *Application* you select. If you want to see all the applications listed, leave *Category* set to *All Categories*.

- 5 Using the *Application* selection, choose the application you want to add.
The applications available to you will be limited to those in the category you select.
- 6 Select the *Action* the FortiGate unit will take when it detects network traffic from the application:

- *Block* will stop all traffic from the application and log all occurrences.
- *Monitor* allows the application traffic to flow normally and log all occurrences.

If you set the action to *Monitor*, you have the option of enabling traffic shaping for the application or applications specified in this application list entry. For more information about application control traffic shaping, see [“Application traffic shaping” on page 203](#)

- *Reset* will reset the network connection on the session that the specified application traffic was detected on.
- 7 Enable *Session TTL* to specify a time-to-live value for the session, in seconds. If this option is not enabled, the TTL defaults to the setting of the CLI command `config system session-ttl`.
 - 8 Select *Enable Packet Log* to have the FortiGate unit save the packets that application control used to determine the traffic came from the application.
 - 9 Some applications have additional options:

IM Options (for some IM applications)	
Block Login	Select to prevent users from logging in to the selected IM system.
Block File Transfers	Select to prevent the sending and receiving of files using the selected IM system.
Block Audio	Select to prevent audio communication using the selected IM system.
Inspect Non-standard Port	Select to allow the FortiGate unit to examine nonstandard ports for the IM client traffic.
Display DLP meta-information on the system dashboard	Select to include meta-information detected for the IM system on the FortiGate unit dashboard.
Other Options	

Command	<p>Some traffic types include a command option. These include FTP.Command, NNTP.Command, POP3.Command, and SMTP.Command. Specify a command that appears in the traffic that you want to block or pass.</p> <p>For example, enter <code>GET</code> as a command in the <i>FTP.Command</i> application to have the FortiGate unit examine FTP traffic for the GET command. Multiple commands can be entered.</p>
Method	<p>A method option is available for HTTP, RTSP, and SIP protocols. Specify a method that appears in the traffic that you want to block or pass.</p> <p>For example, enter <code>POST</code> as a method in the <i>HTTP.Method</i> application to have the FortiGate unit examine HTTP traffic for the POST method. Multiple methods can be entered.</p>
Program Number	<p>Enter the program number appearing in Sun Remote Procedure Calls (RPC) that you want to block or pass. Multiple program numbers can be entered.</p>
UUID	<p>Enter the UUID appearing in Microsoft Remote Procedure Calls (MSRPC) that you want to block or pass. Multiple UUIDs can be entered.</p>

To add an application filter to an application sensor

- 1 Go to *UTM Profiles > Application Control > Application Sensor*.
- 2 Select an application sensor from the drop-down list in the Edit Application Sensor window title bar.
- 3 Select the *Create New* drop-down icon in the sensor and choose *Filter*.
- 4 Configure the filter that you require. Applications matching all of the characteristics you specify in the filter will be included in the filter.

Category	<p>Select <i>Specify</i> and choose an application category to include in the filter. All applications within the category will be included. Some categories have one or more subcategories to allow you to narrow the included applications. For example, selecting IM will include all of the instant messaging applications, but the VoIP subcategory will restrict the applications to only those related to VoIP.</p> <p>If you select <i>All</i>, the category attribute will not be used to determine which signatures are included in the filter.</p>
Vendor	<p>Select <i>Specify</i> and choose a vendor to include all of that vendor's applications in the filter.</p> <p>If you select <i>All</i>, the vendor attribute will not be used to determine which signatures are included in the filter.</p>

Behavior	<p>Select <i>Specify</i> and choose the type of application behavior to include. For example, selecting <i>Encrypted-Tunneling</i> will include all applications providing or related to encrypted tunneling.</p> <p>If you select <i>All</i>, the behavior attribute will not be used to determine which signatures are included in the filter.</p>
Technology	<p>Select <i>Specify</i> and choose the technology of the applications to include. Options include web-browser, peer-to-peer, client, and server.</p> <p>If you select <i>All</i>, the technology attribute will not be used to determine which signatures are included in the filter.</p>
Protocol	<p>Select <i>Specify</i> and choose the network protocols the applications use.</p> <p>If you select <i>All</i>, the Protocol attribute will not be used to determine which signatures are included in the filter.</p>
Tags	<p>Tags are a means by which you can apply customized labels to your application filters. Specified tags are displayed only within the filter itself on the Edit Application Filter page.</p> <p>By default, the tag feature is disabled on all but the largest FortiGate models. If the Tags option is not visible, you must go to <i>System > Admin > Settings</i> and enable <i>Display Object Tagging and Coloring</i> to enable it.</p> <p>For more information about tags, see the System Administration Guide.</p>
Applied Tags	Displays the tags that you have applied to the filter.
Add tags	Enter a tag and then select the plus (+) icon to add the tag to the filter. This also adds the tag to the <i>Applied tags</i> list.
View Matched rules	Select view a list of all the applications included in the filter with the current settings.
Action	<p>Select the <i>Action</i> the FortiGate unit takes when it detects network traffic from the application:</p> <ul style="list-style-type: none"> • <i>Block</i> will stop all traffic from the application and log all occurrences. • <i>Monitor</i> allows the application traffic to flow normally and log all occurrences. • <i>Reset</i> will reset the network session the application is using. <p>If you set the action to <i>Monitor</i>, you have the option of enabling traffic shaping for the application or applications specified in this application list entry. For more information about application control traffic shaping, see “Application traffic shaping” on page 203.</p>

Session TTL	Enable <i>Session TTL</i> to specify a time-to-live value for the session, in seconds. If this option is not enabled, the TTL defaults to the setting of the CLI command <code>config system session-ttl</code> .
Packet Logging	Select to enable packet logging for the filter. When you enable packet logging on a filter, the unit saves a copy of the packets that match any signatures included in the filter. The packets can be analyzed later. For more information about packet filtering, see “Viewing and saving logged packets” on page 280

5 Select **OK**.

The filter is created and added to the filter list.

Understanding the default application sensor

A default application sensor is provided with your FortiGate unit. You can use it as provided, or modify it as required.



Before using the default application sensor, examine it closely to ensure you understand how it works.

monitor-all	This sensor allows all application traffic and enables the application control monitoring for all traffic.
--------------------	--

Viewing and searching the application list

Go to *UTM Profiles > Application Control > Application List* to view the list of applications the FortiGate unit recognizes. You may find applications by paging manually through the list, apply filters, or by using the search field.

Searching manually

Applications are displayed in a paged list, with 50 applications per page. The bottom of the screen shows the current page and the total number of pages. You can enter a page number and press enter, to skip directly to that page. Previous Page and Next Page buttons move you through the list, one page at a time. The First Page and Last Page button take you to the beginning or end of the list.

Applying application list filters

You can enter criteria for one or more columns, and only the applications matching all the conditions you specify will be listed.

To apply filters

- 1 Go to *UTM Profiles > Application Control > Application List*.
- 2 Select *Filter Settings*.
- 3 Select *Add New Filter*.
- 4 Select column by which to filter.
- 5 Select the item or items by which to filter.
- 6 Continue to add more filters to narrow your search, if required.

7 Select OK.

The options available to you will vary by column. For example, Category allows you to choose one option from a list, while Behavior allows you to select multiple items. Filtering by name allows you to enter a text string and all application names containing the string will be displayed.

Using the search field

To use the search field, located above the application list, start typing any portion of the application name. Application names matching the text you enter are displayed in a drop-down list. A maximum of ten matches are displayed at a time.

Select an application from the drop-down list to display its application list entry.

Application traffic shaping

You can apply traffic shaping for application list entries you configure to pass. Traffic shaping enables you to limit or guarantee the bandwidth available to the application or applications specified in an application list entry. You can also prioritize traffic by using traffic shaping.

When the action is set to *Monitor*, two options appear: *Traffic Shaping* and *Reverse Direction Traffic Shaping*. When enabled, you can select traffic shapers configured in *Firewall Objects > Traffic Shaper*.

You can create or edit traffic shapers by going to *Firewall Objects > Traffic Shaper > Shared*. Per-IP traffic shapers are not available for use in application traffic shaping.

For more information about traffic shaping, see the [Traffic Shaping User Guide](#).

Enabling application traffic shaping

Enabling traffic shaping in an application sensor involves selecting the required shaper. You can create or edit shapers in *Firewall Objects > Traffic Shaper > Shared*.

To enable traffic shaping

- 1** Go to *UTM Profiles > Application Control > Application Sensor*.
- 2** Select an application sensor from the drop-down list in the Edit Application Sensor window title bar.
- 3** Select the application control list entry and choose *Edit*.
- 4** Select *Traffic Shaping* and choose the required traffic shaper from the list.
If the action is set to *Block*, the traffic shaping option is not available. Only allowed traffic can be shaped.
- 5** Select *Reverse Direction Traffic Shaping* and choose the required traffic shaper from the list if traffic flowing in the opposite direction also requires shaping.
- 6** Select *OK*.

Any security policy with this application sensor selected will shape application traffic according to the applications specified in the list entry and the shaper configuration.

Reverse direction traffic shaping

To enable traffic shaping, you must set the action to *Monitor*, enable *Traffic Shaping* and then choose the shaper. This will apply the shaper configuration to the application traffic specified in the entry, but only in the direction as specified in the security policy in which the application sensor is selected. To shape traffic travelling in the opposite direction, enable *Reverse Direction Traffic Shaper*.

For example, if you find that your network bandwidth is being overwhelmed by streaming HTTP video, one solution is to limit the bandwidth by applying a traffic shaper to an application control entry that allows the HTTP.Video application. Your users access the Web using a security policy that allows HTTP traffic from the internal interface to the external interface. Firewall policies are required to initiate communication so even though web sites respond to requests, a policy to allow traffic from the external interface to the internal interface is not required for your users to access the Web. The internal to external policy allows them to open communication sessions to web servers, and the external servers can reply using the existing session.

If you enable *Traffic Shaping* and select the shaper in an application sensor specified in the security policy, the problem will continue. The reason is the shaper you select for *Traffic Shaping* is applied only to the application traffic moving in the direction stated in the security policy. In this case, that is from the internal interface to the external interface. The security policy allows the user to visit the web site and start the video, but the video itself is streamed from the server to the user, or from the external interface to the internal interface. This is the reverse of the direction specified in the security policy. To solve the problem, you must enable *Reverse Direction Traffic Shaping* and select the shaper.

Shaper re-use

Shapers are created independently of firewall policies and application sensors so you are free to reuse the same shapers in multiple list entries and policies. Shared shapers can be configured to apply separately to each security policy or across all policies. This means that if a shaper is configured to guaranteed 1000 KB/s bandwidth, each security policy using the shaper will have its own 1000 KB/s reserved, or all of the policies using the shaper will share a pool of 1000 KB/s, depending on how it is configured.

The same thing happens when a shaper is used in application sensors. If an application sensor using a shaper is applied to two separate policies, how the bandwidth is limited or guaranteed depends on whether the shaper is set to apply separately to each policy or across all policies. In fact, if a shaper is applied directly to one security policy, and it is also included in an application sensor that is applied to another security policy, the same issue occurs. How the bandwidth is limited or guaranteed depends on the shaper configuration.

If a shaper is used more than once within a single application sensor, all of the applications using the shaper are restricted to the maximum bandwidth or share the same guaranteed bandwidth.

For example, you want to limit the bandwidth used by Skype and Facebook chat to no more than 100 KB/s. Create a shaper, enable *Maximum Bandwidth*, and enter 100. Then create an application sensor with an entry for Skype and another entry for Facebook chat. Apply the shaper to each entry and select the application sensor in the security policy that allows your users to access both services.

This configuration uses the same shaper for each entry, so Skype **and** Facebook chat traffic are limited to no more than 100 KB/s in total. That is, traffic from both applications is added and the total is limited to 100 KB/s. If you want to limit Skype traffic to 100 KB/s and Facebook chat traffic to 100 KB/s, you must use separate shapers for each application control entry.

Application control monitor

The application monitor enables you to gain an insight into the applications generating traffic on your network. When monitor is enabled in an application sensor entry and the list is selected in a security policy, all the detected traffic required to populate the selected charts is logged to the SQL database on the FortiGate unit hard drive. The charts are available for display in the executive summary section of the log and report menu.



Because the application monitor relies on a SQL database, the feature is available only on FortiGate units with an internal hard drive.

While the monitor charts are similar to the top application usage dashboard widget, it offers several advantages. The widget data is stored in memory so when you restart the FortiGate unit, the data is cleared. Application monitor data is stored on the hard drive and restarting the system does not affect old monitor data.

Application monitor allows you to choose to compile data for any or all of three charts: top ten applications by bandwidth use, top ten media users by bandwidth, and top ten P2P users by bandwidth. Further, there is a chart of each type for the traffic handled by each security policy with application monitor enabled. The top application usage dashboard widget shows only the bandwidth used by the top applications since the last system restart.

Enabling application control monitor

Once you have configured and enabled application control, you can enable application monitor. There are three steps, as detailed below: enabling application monitor in an application sensor, selecting the charts in the security policy, and displaying the charts in the Executive Summary.

To enable application control monitor in an application sensor

- 1 Go to *UTM Profiles > Application Control > Application Sensor*.
- 2 Select an application sensor from the drop-down list in the Edit Application Sensor window title bar.
- 3 Select *Enable Monitoring*.
- 4 Select *OK*.

With application control monitoring enabled, the FortiGate unit begins collecting data for the applications specified in the application sensor from the traffic handled by all policies using the list. If you require monitoring in other application sensors, follow the same procedure to enable it in each sensor.

To configure the charts for which data is collected

- 1 Go to *Policy > Policy > Policy*.
- 2 Select the security policy in which the application sensor is selected and choose *Edit*. Note the security policy ID number.
- 3 Under *UTM*, the *Enable Application Control* selection has three new options, one for each chart type. Select one or more chart types.
- 4 Select *OK*.

- 5 If you have the application sensor specified in multiple firewall policies, repeat this procedure for each policy.

For more information about executive summary charts, see the [Logging and Reporting User Guide](#).

To display the application monitor charts

- 1 Go to *Log&Report > Report Access > Executive Summary*.
- 2 Select *Add Widget*.
- 3 Select the chart you want from the *Widgets* list.

The three application monitor charts correspond to the three chart selections in the security policy. They are listed in the list as:

- top10-application-bw-X-0
- top10-media-user-X-0
- top10-p2p-user-bw-X-0

If you have application monitor enabled in multiple firewall policies, one chart of each type per policy will be available for you to choose. The 'x' in the chart name is the security policy number.

- 4 Select a *Daily* or *Weekly* schedule. The chart will display the data collected from only the current day or current week, depending on the setting. The chart will be reset daily on the hour specified, or weekly on the hour and day specified.
- 5 Select *OK*.

Application control packet logging

Packet logging saves the network packets that application control identifies application traffic with. These packets can be used to trouble-shoot false positives or for forensic investigation. The FortiGate unit saves the logged packets to the attack log, wherever the logs are configured to be stored, whether memory, internal hard drive, a FortiAnalyzer unit, or the FortiGuard Analysis and Management Service.

You can enable packet logging in individual application list entries. Use caution in enabling packet logging. Application sensor entries configured with few restrictions can contain hundreds of applications, potentially resulting in a flood of saved packets. This would take up a great deal of space, require time to sort through, and consume considerable system resources to process. Packet logging is designed as a focused diagnostic tool and is best used with a narrow scope.



Although logging to multiple FortiAnalyzer units is supported, packet logs are not sent to the secondary and tertiary FortiAnalyzer units. Only the primary unit receives packet logs.

To enable application control packet logging

- 1 Create an entry in an application sensor. For more information, see [“Adding applications to an application sensor” on page 198](#).
- 2 Before saving the entry, select *Packet Log*.
- 3 Select the application sensor in the security policy that allows the network traffic the FortiGate unit will examine for the application or applications.

For information on viewing and saving logged packets, see [“Viewing and saving logged packets” on page 280](#).

Application considerations

Some applications behave differently from most others. You should be aware of these differences before using application control to regulate their use.

IM applications

Application control regulates most instant messaging applications by preventing or allowing user access to the service. Selecting *Block Login* will not disconnect users who are logged in when the change is made. Once users log out, however, they will not be able to log in again.

Skype

Based on the NAT firewall type, Skype takes advantage of several NAT firewall traversal methods, such as STUN (Simple Traversal of UDP through NAT), ICE (Interactive Connectivity Establishment) and TURN (Traversal Using Relay NAT), to make the connection.

The Skype client may try to log in with either UDP or TCP, on different ports, especially well-known service ports, such as HTTP (80) and HTTPS (443), because these ports are normally allowed in firewall settings. A client who has previously logged in successfully could start with the known good approach, then fall back on another approach if the known one fails.

The Skype client could also employ Connection Relay. This means if a reachable host is already connected to the Skype network, other clients can connect through this host. This makes any connected host not only a client but also a relay server.

Application control examples

Blocking all instant messaging

Instant messaging use is not permitted at the Example Corporation. Application control helps enforce this policy.

First you will create an application sensor with a single entry that includes all instant messaging applications. You will set the list action to block.

To create the application sensor

- 1 Go to *UTM Profiles > Application Control > Application Sensor*.
- 2 Select the *Create New* icon in the title bar of the *Edit Application Sensor* window.
- 3 In the *Name* field, enter `no IM` for the application sensor name.
- 4 Select *OK*.
- 5 Select the *Create New* drop-down icon in the sensor and choose *Entry*.
- 6 For *Category*, select *im*.
- 7 For *Action*, select *Block*.
- 8 Select *OK* to save the new list entry.
- 9 Select *OK* to save the list.

Next you will enable application control and select the list.

To enable application control and select the application sensor

- 1 Go to *Policy > Policy > Policy*.
- 2 Select the security policy that allows the network users to access the Internet and choose *Edit*.
- 3 Enable *UTM*.
- 4 Select *Enable Application Control*.
- 5 Select the *no IM* application sensor.
- 6 Select *OK*.

No IM use will be allowed by the security policy. If other firewall policies handle traffic that users could use for IM, enable application control with the *no IM* application sensor for those as well.

Allowing only software updates

Some departments at Example Corporation do not require access to the Internet to perform their duties. Management therefore decided to block their Internet access. Software updates quickly became an issue because automatic updates will not function without Internet access and manual application of updates is time-consuming.

The solution is configuring application control to allow only automatic software updates to access the Internet.

To create an application sensor — web-based manager

- 1 Go to *UTM Profiles > Application Control > Application Sensor*.
- 2 Select the *Create New* icon in the title bar of the *Edit Application Sensor* window.
- 3 In the *Name* field, enter `Updates_Only` as the application sensor name.
- 4 Select *OK*.
- 5 Select the *Create New* drop-down icon in the sensor and choose *Entry*.
- 6 Select *update* from the *Category* list.
- 7 Select *Pass* from the *Action* list.
- 8 Select *OK* to save the entry.

This application list entry will allow all software update application traffic.

- 9 Select the *All Other Known Applications* entry.
- 10 Select *Edit*.
- 11 Select *Block* from the *Action* list.
- 12 Select *OK*.

This application list entry will block all traffic from recognized applications that are not specified in this application sensor.

- 13 Select the *All Other Unknown Applications* entry.
- 14 Select *Edit*.
- 15 Select *Block* from the *Action* list.
- 16 Select *OK*.

This application list entry will block all traffic from applications that are not recognized by the application control feature.

- 17 Select *OK*.
- 18 Select *OK* to save the application sensor.

To create an application sensor — CLI

```
config application list
  edit Updates_Only
    config entries
      edit 1
        set category 17
        set action pass
      end
    set other-application-action block
    set unknown-application-action block
  end
```

Selecting the application sensor in a security policy

An application sensor directs the FortiGate unit to scan network traffic only when it is selected in a security policy. When an application sensor is selected in a security policy, its settings are applied to all the traffic the security policy handles.

To select the application sensor in a security policy — web-based manager

- 1 Go to *Policy > Policy > Policy*.
- 2 Select a policy.
- 3 Select the *Edit* icon.
- 4 Enable *UTM*.
- 5 Select the *Enable Application Control* option.
- 6 Select the *Updates_only* list.
- 7 Select *default* from the *Protocol Options* list.

Application control can not be enabled without selecting a protocol options profile. A default profile is provided.

- 8 Select *OK*.

To select the application sensor in a security policy — CLI

```
config firewall policy
  edit 1
    set utm-status enable
    set profile-protocol-options default
    set application-list Updates_Only
  end
```

Traffic handled by the security policy you modified will be scanned for application traffic. Software updates are permitted and all other application traffic is blocked.

Application Control interface reference

This section describes how to configure the application control options associated with firewall policies.

By using the UTM feature's application control, the unit can detect and take action against network traffic depending on the application generating the traffic. Based on Intrusion Protection protocol decoders, application control is a more user-friendly and powerful way to use Intrusion Protection features to log and manage the behavior of application traffic passing through the unit. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols.

The unit can recognize the network traffic generated by a large number of applications. You can create application control black/white lists that specify the action to take with the traffic of the applications you need to manage and the network on which they are active. Add application control lists to firewall policies applied to the network traffic you need to monitor.

Fortinet is constantly increasing the list of applications that application control can detect by adding applications to the [FortiGuard Application Control Database](#). Because intrusion protection protocol decoders are used for application control, the application control database is part of the [FortiGuard Intrusion Protection System Database](#) and both of these databases have the same version number.

You can find the version of the application control database that is installed on your unit, by going to the *License Information* dashboard widget and find IPS Definitions version.

You can go to the [FortiGuard Application Control List](#) to see the complete list of applications supported by FortiGuard. This web page lists all of the supported applications. You can select any application name to see details about the application.

This topic includes the following:

- [Application Sensor](#)
- [Application List](#)



DiffServ is supported per-application and is available only in the CLI.

Application Sensor

Each application control list contains details about the application traffic to be monitored and the actions to be taken when it is detected. An application control list must be selected in a firewall policy to take effect.

There are no default application control lists provided.

The unit examines network traffic for the application entries in the listed order, one at a time, from top to bottom. Whenever a match is detected, the action specified in the matching rule is applied to the traffic and further checks for application entry matches are stopped. Because of this, you can use both actions to create a complex rule with fewer entries.

Application sensor configuration settings

The following are application sensor configuration settings in *UTM Profiles > Application Control > Application Sensor*.

Application Sensor page Lists each individual black/white list that you created. On this page, you can edit, delete and create a new application sensors. You are redirected to this page when you select <i>View List</i> on the Edit Application Sensor page.	
Create New	Creates a new application control sensor. When you select <i>Create New</i> , you are automatically redirected to the New Application Control List page. This page provides a name field and a comment field. You must enter a name to go to the Edit Application Sensor page where you can then configure settings for the new application sensor.
Edit	Modifies settings within an application black/white list. When you select <i>Edit</i> , you are automatically redirected to the Edit Application Control List page.
Delete	Removes the application control black/white list from within the list on the page.
Name	The available application control lists.
# of Entries	The number of application rules in each application control list.
Comments	An optional description of each application control list.
Ref.	<p>Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a firewall policy; on the Profile page (<i>UTM Profiles > Antivirus > Profile</i>), 1 appears in <i>Ref.</i>.</p> <p>To view the location of the referenced object, select the number in <i>Ref.</i>, and the Object Usage window appears displaying the various locations of the referenced object.</p> <p>To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:</p> <ul style="list-style-type: none"> • View the list page for these objects – automatically redirects you to the list page where the object is referenced at. • Edit this object – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • View the details for this object – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy, and that firewall policy's settings appear within the table.

Edit Application Sensor page Provides settings for configuring the applications for the list. When you are editing a list, you are redirected to this page. Note: Logging is enabled in the CLI.	
Name	If you are editing an existing application control list and want to change the name, enter a new name in the field. You must select <i>OK</i> to save the change.
Comments	If you are editing an existing list and want to change or add a description, enter the new text in the field. You must select <i>OK</i> to save the change.
Create New	<p>Creates a new application entry. When you select <i>Create New</i>, you are automatically redirected to the New Application Filter page.</p> <p>When you select the down arrow beside <i>Create New</i>, you can choose to create either a new application filter or entry.</p> <p>When you select <i>Filter</i>, you are automatically redirected to the New Application Filter page where you can configure a filter.</p> <p>When you select <i>Entry</i>, you are automatically redirected to the New Application Entry page where you can configure an entry.</p>
Edit	Modifies settings within the application control entry. When you select <i>Edit</i> you are automatically redirected to the Edit Application Entry page.
Delete	<p>Removes the application control entry in the list.</p> <p>To remove multiple application control entries from within the list, on the Edit Application Sensor page, in each of the rows of the entries you want removed, select the check box and then select <i>Delete</i>.</p> <p>To remove all application control entries from the list, on the Edit Application Sensor page, select the check box in the check box column and then select <i>Delete</i>.</p>
Insert	Creates a new application control entry above the entry you highlighted. When you select <i>Insert</i> , you are automatically redirected to the New Application Entry page.
Move To	<p>Moves the application control entry to any position in the list. When you select <i>Move To</i>, the Move Application Control Entry window appears.</p> <p>To move an application control entry, select the new position <i>Before</i> or <i>After</i>, which will place the current entry before or after the entry you enter in the <i>Application ID</i> field. Use the number found in the <i>ID</i> column when entering the new position in the <i>Application ID</i> field.</p>
View Rules	Select to view the rules of an entry. When you select <i>View Rules</i> , the Matched Rules window appears. You can view all the rules associated within that entry in this window.
Page Controls	Use to navigate through the application control entries within an application control list.
ID	The identification number of the entry.

Category	<p>The category indicates the scope of the applications included in the application entry if <i>Application</i> is set to <i>all</i>. For example, if <i>Application</i> is <i>all</i> and <i>Category</i> is <i>toolbar</i>, then all the toolbar applications are included in the application entry even though they are not specified individually.</p> <p>If <i>Application</i> is a single application, the value in <i>Category</i> has no effect on the operation of the application entry.</p>
Vendor	The application's vendor name.
Behavior	The type of behavior chosen.
Technology	The type of technology associated with the application.
Application	<p>The type of application that was chosen.</p> <p>Note: <i>Full List</i> appears in this column only when you choose all applications for a filter. When you select <i>Full List</i>, the Match Rules window appears where you can view all the applications.</p>
Action	If the unit detects traffic from the specified application, the selected action will be taken.
<p>New Application Filter page</p> <p>Provides settings for configuring an application filter to add to the application control sensor.</p> <p>This page appears when you select <i>Create New</i> on the Edit Application Sensor page. If you are on the Application Sensor page, and you select <i>Create New</i>, you will be redirected to the New Application Filter page.</p>	
Category	<p>The applications are categorized by type. If you want to choose an IM application, for example, select the <i>im</i> category, and the application control list will show only the <i>im</i> applications.</p> <p>The <i>Category</i> selection can also be used to specify an entire category of applications. To select all IM applications for example, select the <i>im</i> category, and select <i>all</i> as the application. This specifies all the IM applications with a single application control black/white list entry.</p>
Vendor	Select to either specify a vendor or enable all vendors.
Behavior	When you select <i>Specify</i> , the lists <i>Available</i> and <i>Selected</i> appear. Select the available behavior of the application (for example, encrypted-tunneling) in the <i>Available</i> list and then move it to the <i>Selected</i> list using the -> arrow. Use the same method to remove a behavior from the <i>Selected</i> list except use the <- arrow.
Technology	Select to include all technology or specify the technology. For example, web browsers.
Protocol	Select to include all protocols or specify a particular protocol.
Tags	<p>Adds and displays the tags you create.</p> <p>If tag settings are not available on the web-based manager, you must enable them in <i>System > Admin > Settings</i>.</p>
Applied tags	Displays the current tags configured for the filter.

Add tags	Enter the tag in the field and then select the plus sign (+) beside the field to add the tag to the list in <i>Applied tags</i> .
View Matched rules	Select to view the matched rules.
Action	If the unit detects traffic from the specified application, the selected action will be taken.
Monitor	Select to monitor the filter using traffic shaping or reverse direction traffic shaping or both.
Block	Select to block.
Session TTL	The application's session TTL. If this option is not enabled, the TTL defaults to the setting of the <code>config system session-ttl</code> CLI command.
Packet Logging	Select to log the occurrence of packet logs which concern application control.
New Application Entry page	
Provides settings for configuring an application entry, to add to the application sensor.	
Category	Select a category from the drop-down list.
Application	Select an application from the drop-down list.
Action	Select either <i>Monitor</i> or <i>Block</i> for the type of action the unit will take. When you select <i>Monitor</i> , the options for applying traffic shaping and reverse direction traffic shaping. Select the check box beside either one or both to enable these options and then select
Session TTL	Enter a number for the session's time to live.
Packet Logging	Select to enable packet logging.

Application List

The application list displays applications, which also shows their popularity and risk. You can view the details of each application by selecting the application's name; this link redirects you to the [FortiGuard Application Control List](#) where the details are given for the application. You can also filter the information that appears in *UTM Profiles > Application Control > Application List*.

You can go to the [FortiGuard Application Control List](#) to see the complete list of applications supported by FortiGuard. This web page lists all of the supported applications. You can select any application name to see details about the application.

Application lists are viewed from *UTM Profiles > Application Control > Application List*.

Application List page	
Lists the applications that are available on the unit, which includes their category, popularity rating and risk.	
Tags	<p>Select to add or remove tags to the applications in the list.</p> <p>Note: If <i>Tags</i> is not available on the web-based manager, you must enable it in <i>System > Admin > Settings</i>.</p> <p>When you select the down arrow beside <i>Tags</i>, you can add tags or remove tags.</p> <p>To add tags to an application, select the application first then select the down arrow to then select <i>Add Tags</i>. The Add Tags window appears. Enter the tag in the <i>Add tag</i> field and select the plus (+) sign; repeat until all tags are in the Tags to apply list.</p> <p>To remove tags, select the application first, select the down arrow beside Tags, and then select <i>Remove Tags</i>. The Remove Tags window appears. Select the tags that you want removed in the <i>Applied Tags</i> row; repeat until all the tags are in the <i>Tags to remove</i> row. The tags will automatically be put in the <i>Tags to remove</i> row after being selected in the <i>Applied Tags</i> row.</p> <p>If there are tags that you want to add that have been configured for another object, you can add those tags as well to signatures. To apply these other object tags, select the signature first, select the down arrow beside Tags, and then select <i>Add Tags</i>. The Add Tags window appears. Select the tags you want to add in the <i>Click tag to add</i> row. The tags automatically appear in the <i>Tags to apply</i> row. Select <i>OK</i> to add those tags to the application.</p>
Column Settings	Customize the column view. You can select the columns to hide or display them and specify the column display order.

Filter Settings	<p>Select to filter the information on the page. <i>Filters</i> appears automatically after selecting <i>Filter Settings</i>, below the column headings. Use to configure filter settings.</p> <p>Note: <i>Filter Settings</i> configures all filter settings. Filter icons are used to configure filter settings within that column.</p> <p>To apply a filter setting, select the plus sign beside <i>Add new filter</i> and then select and enter the information required. Repeat to add other filter settings.</p> <p>To modify settings, select <i>Change</i> beside the setting and edit the settings.</p> <p>To clear all filter settings, select the icon beside <i>Clear all filters</i>.</p> <p>To use a filter icon to filter settings within a column, select the filter icon in the column; <i>Filters</i> appears. Within <i>Filters</i>, configure the settings for that column.</p> <p>The <i>Filters Settings</i> on the Application List page contains <i>Copy to Sensor</i>, which allows you to copy filter settings and apply them to an application sensor.</p> <p>To apply existing filter settings to a sensor, select the down arrow beside <i>Filter Settings</i>, and then select <i>Copy to Sensor</i>. The Select Object window appears. Select the sensor that you want to apply the settings to from the drop-down list. Select <i>OK</i>.</p>
Search	Enter search criteria into the field and then press Enter on your keyboard. Use the <i>Clear All</i> icon beside the field to clear the search results.
Page Controls	Use to navigate through the list to view the applications.
[Total: <maximum number>]	The maximum number of applications that are currently in the FortiGuard Application Control List.
Application Name	The name of the application.
Category	The category that the application is associated with.
Vendor	The type of vendor.
Technology	The type of technology that the application uses. For example, 56.COM using Peer-to-Peer technology.
Protocol	The type of protocol the application uses.
Behavior	The type of behavior that is associated with the application.
Tags	<p>The tags that are associated with that application.</p> <p>If no tag configuration settings display, this indicates that this feature is disabled. You can enable tag configuration settings from <i>System > Admin Settings</i>.</p>



DoS policy

Denial of Service (DoS) policies are primarily used to apply DoS sensors to network traffic based on the FortiGate interface it is entering as well as the source and destination addresses. DoS sensors are a traffic anomaly detection feature to identify network traffic that does not fit known or common traffic patterns and behavior. A common example of anomalous traffic is the denial of service attack. A denial of service occurs when an attacking system starts an abnormally large number of sessions with a target system. The large number of sessions slows down or disables the target system, so that legitimate users can no longer use it.

This section describes how to create and configure DoS sensors and policies to protect the publicly accessible servers on your network.

The following topics are included in this section:

- [DoS policy concepts](#)
- [Enable DoS](#)
- [DoS example](#)

DoS policy concepts

DoS policies are similar to firewall policies except that instead of defining the way traffic is allowed to flow, they keep track of certain traffic patterns and attributes and will stop traffic displaying those attributes. Further, DoS policies affect only incoming traffic on a single interface. You can further limit a DoS policy by source address, destination address, and service.

DoS policies examine network traffic very early in the sequence of protective measures the FortiGate unit deploys to protect your network. Because of this early detection, DoS policies are a very efficient defence that uses few resources. Denial of service attacks, for example, are detected and its packets dropped before requiring security policy look-ups, antivirus scans, and other protective but resource-intensive operations. For more information about DoS attacks, see [“Defending against DoS attacks” on page 24](#).

Enable DoS

A DoS policy examines network traffic arriving at an interface for anomalous patterns usually indicating an attack. Enable DoS sensors to protect your FortiGate unit from attack. To apply a DoS policy, you must follow the steps below in sequence:

- 1 Create a DoS sensor.
- 2 Create a DoS policy
- 3 Apply the DoS sensor to the DoS policy.

Creating and configuring a DoS sensor

Because an improperly configured DoS sensor can interfere with network traffic, no DoS sensors are present on a factory default FortiGate unit. You must create your own and then enable them before they will take effect. Thresholds for newly created sensors are preset with recommended values that you can adjust to meet the needs of your network.



It is important to know normal and expected network traffic before changing the default anomaly thresholds. Setting the thresholds too low could cause false positives, and setting the thresholds too high could allow otherwise avoidable attacks.

To create a DoS sensor

- 1 Go to *UTM Profiles > Intrusion Protection > DoS Sensor*.
- 2 Select *Create New*.
- 3 In the *Name* field, enter the name of the DoS sensor.
- 4 Optionally, enter a description of the DoS sensor in the *Comment* field.
- 5 Select *OK*.

The DoS sensor is created and the sensor configuration window appears. However, a newly created DoS sensor contains default values which may not be appropriate for your network. You can adjust these values by configuring the DoS sensor thresholds.

To configure a DoS sensor

- 1 Go to *UTM Profiles > Intrusion Protection > DoS Sensor*.
- 2 Select the DoS sensor you want to configure and choose *Edit*.
- 3 The DoS sensor configuration window appears.

The *Anomalies Configuration* table lists 12 types of network anomalies.

Anomaly	Description
tcp_syn_flood	If the SYN packet rate of new TCP connections, including retransmission, to one destination IP address exceeds the configured threshold value, the action is executed. The threshold is expressed in packets per second.
tcp_port_scan	If the SYN packet rate of new TCP connections, including retransmission, from one source IP address exceeds the configured threshold value, the action is executed. The threshold is expressed in packets per second.
tcp_src_session	If the number of concurrent TCP connections from one source IP address exceeds the configured threshold value, the action is executed.
tcp_dst_session	If the number of concurrent TCP connections to one destination IP address exceeds the configured threshold value, the action is executed.
udp_flood	If the UDP traffic to one destination IP address exceeds the configured threshold value, the action is executed. The threshold is expressed in packets per second.
udp_scan	If the number of UDP sessions originating from one source IP address exceeds the configured threshold value, the action is executed. The threshold is expressed in packets per second.

udp_src_session	If the number of concurrent UDP connections from one source IP address exceeds the configured threshold value, the action is executed.
udp_dst_session	If the number of concurrent UDP connections to one destination IP address exceeds the configured threshold value, the action is executed.
icmp_flood	If the number of ICMP packets sent to one destination IP address exceeds the configured threshold value, the action is executed. The threshold is expressed in packets per second.
icmp_sweep	If the number of ICMP packets originating from one source IP address exceeds the configured threshold value, the action is executed. The threshold is expressed in packets per second.
icmp_src_session	If the number of concurrent ICMP connections from one source IP address exceeds the configured threshold value, the action is executed.
icmp_dst_session	If the number of concurrent ICMP connections to one destination IP address exceeds the configured threshold value, the action is executed.

- 4 Select *Enable* to have the FortiGate unit examine traffic for the anomaly.
- 5 Select *Logging* to create an entry in the attack log if the anomaly is detected.
- 6 Select an *Action* for the anomaly. By default, the action is *Pass*, which allows the traffic containing the anomaly to pass uninterrupted. If set to *Block*, the anomalous traffic is blocked and will not flow through the FortiGate unit.

With a Fortinet security processing module installed, FortiGate units that support these modules offer a third action for the `tcp_syn_flood` threshold. In addition to *Block* and *Pass*, you can choose to *Proxy* connect attempts when their volume exceeds the threshold value. When the `tcp_syn_flood` threshold action is set to *Proxy*, incomplete TCP connections are allowed as normal as long as the configured threshold is not exceeded. If the threshold is exceeded, the FortiGate unit will intercept incoming SYN packets with a hardware accelerated SYN proxy to determine whether the connection attempts are legitimate or a SYN flood attack. Legitimate connections are allowed while an attack is blocked.



Because DoS sensors are configured before being applied to an interface, you can assign a DoS sensor with the *Proxy* action to an interface that does not have hardware SYN proxy support. In this circumstance, the *Proxy* action is invalid and a *Pass* action will be applied.

- 7 Set the *Threshold* value for the anomaly. See the table in step 3 for details about the threshold values for each anomaly.
- 8 Select *OK*.

Creating a DoS policy

DoS policies examine network traffic entering an interface. The DoS sensor specified in the DoS policy allows you to limit certain anomalous traffic to protect against attacks.

To create a DoS policy

- 1 Go to *Policy > Policy > DoS Policy* and select *Create New*.

- 2 For *Source Interface/Zone*, select the interface on which the DoS policy will examine incoming traffic.
- 3 For *Source Address*, select the address or address group that defines the source addresses of the traffic the DoS policy will examine. Network traffic from addresses not included in the selected address group is ignored by this DoS policy.
- 4 For *Destination Address*, select the address or address group that defines the destination addresses of the traffic the DoS policy will examine. Network traffic to addresses not included in the selected address group is ignored by this DoS policy.
- 5 For *Service*, select the type of network traffic the DoS policy will examine. Protocols not included in the selected service or service group are ignored by this DoS policy.
- 6 Select the *DoS Sensor* check box and choose the required sensor from the list.
- 7 Select *OK*.

Apply an IPS sensor to a DoS policy

Although IPS sensors are usually applied to firewall policies, you can also apply them to DoS policies by using CLI commands. There are two reasons you might want to apply an IPS sensor to a DoS policy:

- If you want to have all traffic coming into one FortiGate unit interface checked for the signatures in an IPS sensor, it is simpler to apply the IPS sensor once to a DoS policy. In a complex configuration, there could be many policies controlling the traffic coming in on a single interface.
- The operations in a DoS policy occur much earlier in the sequence of operations performed on incoming traffic. This means that IPS examination of traffic occurs much sooner if the IPS sensor is applied to a DoS policy. Fewer system resources are used because signatures set to block traffic will take effect before security policy checking and all of the scans specified in the security policy.

The CLI command for configuring DoS policies is `config firewall interface-policy`. The following command syntax shows how to add an example IPS sensor called `all_default_pass` to a DoS policy with policy ID 5 that was previously added from the web-based manager.

```
config firewall interface-policy
edit 5
    set ips-sensor-status enable
    set ips-sensor all_default_pass
end
```

DoS example

The Example.com corporation installed a web server and connected it to Port5 on its FortiGate unit. To protect against denial of service attacks, you will configure and apply a DoS sensor to protect the web server.

To create the DoS sensor

- 1 Go to *UTM Profiles > Intrusion Protection > DoS Sensor*.
- 2 Select *Create New*.
- 3 Enter `Web Server` in the *Name* field.
- 4 In the *Anomalies Configuration* table, select the *Enable* check box in the table heading. This enables all the anomalies with a single selection.

- 5 Select *OK* to save the new DoS policy.

As suggested in “[Defending against DoS attacks](#)” on page 24, the IT administrators will run the DoS policy with logging enabled and the anomaly actions set to *Pass* until they determine the correct threshold values for each anomaly.

To create a DoS policy

- 1 Go to *Policy > Policy > DoS Policy*.
- 2 Select *Create New*.
- 3 In the *Source Interface/Zone* field, select *Port1* which is the interface connected to the Internet.
- 4 In the *Source Address* field, select *all*.
- 5 In the *Destination Address* field, select *all*.
If there were more than one publicly accessible server connected to the FortiGate unit, you would specify the address of the web server in this field.
- 6 In the *Service* field, select *ANY*.
- 7 Select the *DoS Sensor* check box and choose *Web Server* from the list.
- 8 Select *OK* to save the DoS policy.

The DoS policy will monitor all network traffic entering Port1 and log the violations if the thresholds in the *Web Server* DoS sensor are exceeded.

DoS Policy interface reference

The DoS security policy list displays the DoS security policies in their order of matching precedence for each interface, source/destination address pair, and service.

If virtual domains are enabled on the unit, DoS security policies are configured separately for each virtual domain; you must access the VDOM before you can configure its security policies.

You can add, delete, edit, and re-order security policies in the DoS policy list. DoS policy order affects security policy matching. As with security policies, DoS security policies are checked against traffic in the order in which they appear in the DoS policy list, one at a time, from top to bottom. When a matching security policy is discovered, it is used and further checking for DoS policy matches are stopped.

The DoS policy configuration allows you to specify the interface, a source address, a destination address, and a service. All of the specified attributes must match network traffic to trigger the security policy.

DoS policies configuration settings

The following are DoS policy configuration settings in *Policy > Policy > DoS Policy*.

DoS Policy page Lists each individual DoS policy that you created. On this page, you can edit, delete or create a new DoS policy.	
Create New	<p>Adds a new DoS policy. Select the down arrow beside <i>Create New</i> to add a new section to the list to visually group the security policies. When you select <i>Create New</i>, (or the <i>Policy</i> option from the down arrow's drop-down list), you are automatically redirected to the New Policy page.</p> <p>When you select <i>Section Title</i>, the Section Title window appears. Enter the section title name in the <i>Name</i> field and then enter the DoS policy ID number of the security policy that you want the section title to come before in the <i>Starting Policy ID</i> field. For example, <i>branch_office_dos</i> comes before the DoS policy ID 2, so 2 is entered in the <i>Starting Policy ID</i> field.</p>
Edit	<p>Modifies settings within the security policy. When you select <i>Edit</i>, you are automatically redirected to the Edit Policy page.</p> <p>When you select the down arrow beside <i>Edit</i>, you can select to modify the security policy (<i>Edit Policy</i>), disable a security policy (<i>Disable</i>), or enable a security policy (<i>Enable</i>).</p>
Delete	<p>Removes a security policy from the list on the DoS Policy page.</p> <p>To remove multiple DoS security policies from within the list, on the DoS Policy page, in each of the rows of the security policies you want removed, select the check box and then select <i>Delete</i>.</p> <p>To remove all DoS security policies from the list, on the DoS Policy page, select the check box in the check box column, and then select <i>Delete</i>.</p>
Move To	<p>Moves the corresponding security policy before or after another security policy in the list.</p> <p>When you select <i>Move To</i>, the Move Policy window appears. To move a security policy, select the new position either <i>Before</i> or <i>After</i>, which will place the current entry before or after the security policy number that you enter in the (<i>Policy ID</i>) field. Enter the security policy ID number and then select OK. For example, policy ID 2 is moved after policy ID 5.</p>
Insert	<p>Inserts a new security policy above the corresponding security policy. When you select Insert, the New Policy window appears.</p>

Filter Settings	<p>Select to filter the information on the page. <i>Filters</i> appears automatically after selecting <i>Filter Settings</i>, below the column headings. Use to configure filter settings.</p> <p>Note: <i>Filter Settings</i> configures all filter settings. Filter icons are used to configure filter settings within that column.</p> <p>To apply a filter setting, select the plus sign beside <i>Add new filter</i> and then select and enter the information required. Repeat to add other filter settings.</p> <p>To modify settings, select <i>Change</i> beside the setting and edit the settings.</p> <p>To clear all filter settings, select the icon beside <i>Clear all filters</i>.</p> <p>To use a filter icon to filter settings within a column, select the filter icon in the column; <i>Filters</i> appears. Within <i>Filters</i>, configure the settings for that column.</p>
Column Settings	Customize the table view. You can select the columns to hide or display and specify the column displaying order in the table.
Section View	Select to display security policies organized by interface.
Global View	Select to list all security policies in order according to a sequence number.
ID	A unique identifier for each security policy. Policies are numbered in the order they are created.
Source	The source address or address group to which the security policy applies.
Destination	The destination address or address group to which the security policy applies.
Service	The service to which the security policy applies.
DoS Sensor	The DoS sensor selected in this security policy.
Interface	The interface to which this security policy applies.
Status	When selected, the DoS security policy is enabled. Clear the check box to disable the security policy.
New Policy page Provides settings for configuring a DoS security policy. When you select <i>Create New</i> on the DoS Policy page, you are automatically redirected to this page.	
Source Interface/Zone	The interface or zone to be monitored.
Source Address	Select an address, address range, or address group to limit traffic monitoring to network traffic sent from the specified address or range. Select <i>Multiple</i> to include multiple addresses or ranges. You can also select <i>Create New</i> to add a new address or address group.
Destination Address	Select an address, address range, or address group to limit traffic monitoring to network traffic sent to the specified address or range. Select <i>Multiple</i> to include multiple addresses or ranges. You can also select <i>Create New</i> to add a new address or address group.

Service	Select a firewall pre-defined service or a custom service to limit traffic monitoring to only the selected service or services. You can also select <i>Create New</i> to add a custom service.
DoS Sensor	Select and specify a DoS sensor to have the Fortinet unit apply the sensor to matching network traffic. You can also select <i>Create New</i> to add a new DoS Sensor. See “Creating and configuring a DoS sensor” on page 218 .



Endpoint Control and monitoring

This section describes the Endpoint Control feature and how to configure it.

The following topics are included in this section:

- [Endpoint Control overview](#)
- [Configuring FortiClient required version and download location](#)
- [About application detection and control](#)
- [Creating an endpoint control profile](#)
- [Enabling Endpoint Control in firewall policies](#)
- [Monitoring endpoints](#)
- [Modifying Endpoint Security replacement pages](#)
- [Example](#)

Endpoint Control overview

Endpoint Control ensures that workstation computers (endpoints) meet security requirements, otherwise they are not permitted access. Endpoint Control can enforce

- use of FortiClient Endpoint Security
- use of a licensed version of FortiClient Endpoint Security
- use of FortiClient firewall
- use of FortiClient antivirus protection
- use of FortiClient web content filtering
- use of up-to-date FortiClient antivirus signatures
- installation or running of specific applications
- absence or non-use of specific applications

Non-compliant endpoints can be either warned or blocked.

Of the features listed above, enforcement of FortiClient licensing and FortiClient web content filtering can be configured only through the CLI using the `config endpoint-control profile` command.

Endpoint Control settings are grouped into one or more Endpoint Control profiles. You enable Endpoint Security in firewall policies and select an Endpoint Control profile.

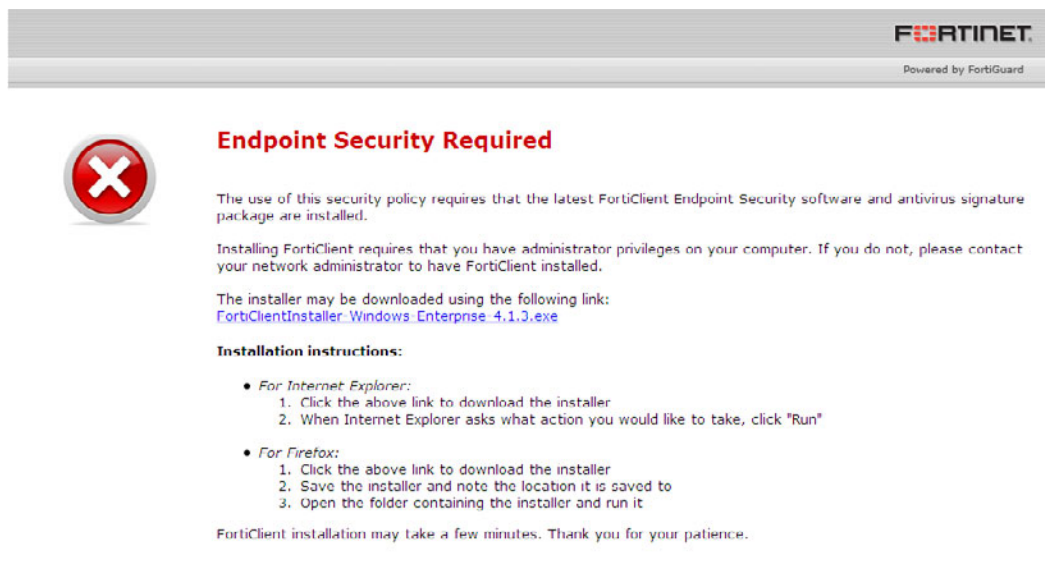
User experience

Endpoint Control applies to users attempting to make a connection that is controlled by a firewall policy with Endpoint Security enabled. The user of a non-compliant endpoint using a web browser receives a replacement message HTML page from the FortiGate unit. The message explains the non-compliance. Depending on the endpoint profile, the user may be allowed to continue or is blocked from further access. For information about modifying these replacement pages, see [“Modifying Endpoint Security replacement pages” on page 236](#).

FortiClient version non-compliance

If the *FortiClient* application detection entry in the Endpoint Control profile has either the Warn or Block action selected, the user sees a message like this:

Figure 10: Default FortiClient non-compliance message



If there is a FortiClient installer available for the user's endpoint computer, a link is provided to download the installer from the location defined in *UTM Profiles > Endpoint Control > Client Installers*. If there is no installer available, the user is asked to contact the network administrator.

If the action on the *FortiClient* application detection entry is Warn, there is a link at the bottom of the page to enable the user to continue to the requested web site without installing FortiClient Endpoint Security. Otherwise, the same message will be displayed for every connection attempt where Endpoint Security is in effect until the user installs FortiClient Endpoint Security.

Blocked user - FortiClient features not compliant

If the Endpoint Control profile has the *Block* action selected for FortiClient features such as antivirus or firewall, the FortiGate unit sends a message like this to the user's browser.:

Figure 11: Endpoint blocked message



The user needs to resolve the listed issues and retry the connection.

Configuration overview

Endpoint Control requires that all hosts using the firewall policy have the FortiClient Endpoint Security application installed. Make sure that all hosts affected by this policy are able to install this application. Currently, FortiClient Endpoint Security is available for Microsoft Windows (2000 and later) only.

To set up Endpoint Control, you need to

- Enable Central Management by the FortiGuard Analysis & Management Service if you will use FortiGuard Services to update the FortiClient application or antivirus signatures. You do not need to enter account information. See “Centralized Management” in the System Administration chapter of the FortiOS Handbook.
- Configure the minimum required version of FortiClient and the location from which non-compliant endpoints can download the FortiClient installer. See “[Configuring FortiClient required version and download location](#)” on page 227.
- Create an endpoint control profile or use a predefined profile. See “[About predefined profiles](#)” on page 230.
- If needed, modify the profile’s predefined FortiClient application detection rules. You can select the action to take on endpoints that do not have FortiClient Endpoint Security and you can set conditions and actions regarding FortiClient features.
- Configure application detection rules for other applications that are required, allowed, or not allowed on endpoints. See “[About application detection and control](#)” on page 229.
- Enable Endpoint Security in firewall policies, selecting the appropriate Endpoint Control profile.



You cannot enable Endpoint in firewall policies if *Redirect HTTP Challenge to a Secure Channel (HTTPS)* is enabled in *User > User > Authentication*.

- Optionally, modify the inactivity timeout for endpoints. The default is 5 minutes. After that time period, the FortiGate unit rechecks the endpoint for Endpoint compliance. To change the timeout, adjust the `compliance-timeout` value in the `config endpoint-control settings` CLI command.
- Optionally, modify the *Endpoint NAC Download Portal* and the *Endpoint NAC Recommendation Portal* replacement messages.

Configuring FortiClient required version and download location

The Endpoint Control feature can set a minimum FortiClient version that endpoints are required to run. To make this policy easy for users, you can configure a download source for the FortiClient installer.

Configuring FortiClient requirement and download location - web-based manager

- 1 Go to *UTM Profiles > Endpoint Control > Client Installers*.

Figure 12: Configuring FortiClient version requirements and installer source

FortiClient Endpoint Security

Information

FortiGuard Availability	✓
FortiClient Endpoint Versions	
Windows Installer	4.1.3 (Updated 2010-04-07) [Download]
AV Signature Package	11.670 (Updated 2010-04-07)
Application Signature Package	1.169 (Updated 2010-04-07)
FortiClient Downloads	0

[Update Now](#)

FortiClient Installer Download Location

The remediation portal will direct users to download from:

☒ FortiGuard Distribution Network

☐ This FortiGate

☐ Custom URL:

FortiClient Version

☒ Enforce Minimum Version (If enabled in Endpoint Profiles)

[Apply](#)

2 Do one of the following:

- Select *FortiGuard Distribution Network*. FortiGuard must be configured on the FortiGate unit.
- Select *This FortiGate*. Users can download a FortiClient installer file from this FortiGate unit. This option is available only on FortiGate models that support upload of FortiClient installer files.
- Select *Custom URL*. Enter the URL from which users can download the FortiClient installer.



Select *This FortiGate* or *Custom URL* if you want to provide a customized FortiClient application. This is required if a FortiManager unit will centrally manage FortiClient applications. For information about customizing the FortiClient application, see the [FortiClient Administration Guide](#).

3 Optionally, select *Enforce Minimum Version* and select the minimum acceptable version number or *Latest Available* for the FortiClient Endpoint Security application.

The list contains the FortiClient versions available from the selected *FortiClient Installer Download Location*.

Fortinet recommends that administrators wait for a reasonable period of time after deploying a FortiClient version update before updating the minimum version required to the most recent version. This gives users some time to install the update.

Configuring FortiClient requirement and download location - CLI

In this example, users are required to have FortiClient version 4.1.3 or later. FortiGuard provides the FortiClient installer.

```
config endpoint-control settings
  set enforce minimum-version enable
  set version-check minimum
  set version 4.1.3
  set download-location fortiguard
end
```

About application detection and control

In firewall policies you can select an endpoint control profile. The application detection list within the endpoint control profile allows or denies endpoint access to the network based on the applications that are installed or running on the endpoint.

The application detection list contains rules specific to individual applications, application vendors, and application categories. A rule tests for a particular condition of the application on the endpoint, which can be any of the following:

- *Installed* — application is installed and may or may not be currently running
- *Not Installed* — application is not installed
- *Running* — application is installed and currently running
- *Not Running* — application is not currently running or is not installed

The rule determines the action to take when the specified application matches the condition. The possible actions are:

- *Allow* — Allow the endpoint to connect.
- *Block* — Block the endpoint.
- *Warn* — Warn the endpoint, but then allow the user to connect.
- *Monitor* — Allow the endpoint to connect and include this endpoint's information in statistics and logs on the Endpoint Monitor page.

FortiClient application rules

There are three application rules for FortiClient that are present in every endpoint control profile: FortiClient, FortiClient AV, and FortiClient Firewall. You can edit, but not delete, these entries.

- **FortiClient** — **Select** the Block, Warn, or Monitor action to apply if the FortiClient application is not installed or not running on the endpoint.
- **FortiClient AV** — **Select** whether to allow or block endpoints that are not running the antivirus feature of the FortiClient application. Optionally, you can also apply this rule to endpoints with an outdated FortiClient antivirus database.
- **FortiClient Firewall** — **Select** whether to allow or block endpoints that are not running the firewall feature of the FortiClient application.

Other application rules

Application detection rules (entries) are based on application signatures provided by FortiGuard Services. You create your application detection list entries by selecting applications from FortiGuard-supplied lists of categories, vendors, and application names. To view application information from FortiGuard services, go to *UTM Profiles > Endpoint Control > Application Database*.

An application detection rule checks applications against the database from the top down until it finds a match. Specific entries, such as those that list one particular application, should precede more general entries, such as those that match all applications of a particular category.

The All application rule

At the bottom of every application detection list is the All rule. This specifies the action to apply to an endpoint with an application installed that does not match a rule higher in the list. The default action is Monitor. If you select Block, endpoints can have only a specific set of applications installed and are denied access if any other applications are installed.

About predefined profiles

Each VDOM has the following default endpoint profiles:

Enforce_FortiClient_AV — **blocks** endpoints without FortiClient Endpoint Security or not running FortiClient antivirus protection. Endpoints with other applications installed are monitored.

P2P_application_detection — **blocks** endpoints running peer-to-peer file sharing. Users whose endpoint does not have FortiClient Endpoint Security installed receive a warning.

Recommend_FortiClient — **monitors** endpoints and presents a warning to users whose endpoint does not have FortiClient Endpoint Security installed.

You can modify or delete these endpoint profiles.

Creating an endpoint control profile

An endpoint profile defines requirements for FortiClient Endpoint Security and other applications on endpoints. The profile is selected in firewall policies and applies to all users of the firewall policy.

To create an endpoint control profile - web-based manager

- 1 Go to *UTM Profiles > Endpoint Control > Profile* and select *Create New*.
- 2 Enter a *Name* and optionally *Comments* for the profile, then select *OK*.
The profile opens, showing the application detection list. There are default entries for FortiClient Endpoint Security with default settings.
- 3 Configure FortiClient-related entries as needed.
- 4 Create additional application detection entries as needed.
- 5 Select *OK*.

To create an endpoint control profile - CLI

```
config endpoint-control profile
  edit profile1
end
```

Setting endpoint FortiClient requirements

Every endpoint control profile requires that FortiClient Endpoint Security must be installed on all endpoints. You can choose whether non-compliant endpoints are blocked, warned, or simply monitored. By default they are blocked.

You can choose whether to require the use of FortiClient antivirus, firewall, or web filtering features. By default, endpoints are not required to use these features.

You can also choose whether to require each endpoint's FortiClient application to be licensed. This is not required by default.

To set the action for endpoints not running FortiClient - web-based manager

- 1 Go to *UTM Profiles > Endpoint Control > Profile* and open the profile for editing.

- 2 Edit the *FortiClient* application detection entry and select the required action: *Block*, *Warn*, or *Monitor*.

For information about these actions, see [“About application detection and control” on page 229](#).

To set the action for endpoints not running FortiClient - CLI

In this example, endpoints that do not have FortiClient Endpoint Security installed will be blocked. The other options for `recommendation-disclaimer` are `enable` to warn the endpoint and `skip` to simply monitor the endpoint.

```
config endpoint-control profile
edit profile1
set recommendation-disclaimer disable
end
```

To require endpoints to use FortiClient antivirus protection - web-based manager

- 1 Go to *UTM Profiles > Endpoint Control > Profile* and open the profile for editing.
- 2 Edit the *FortiClient AV* application detection entry.
- 3 In *Condition*, select *Not Running* to enforce use the antivirus feature, To also require use of an up-to-date AV database, select *Not Running or Up-to-date*.
- 4 In *Action*, select *Block*.
- 5 Select *OK*.

To require endpoints to use FortiClient antivirus protection - CLI

In this example, endpoint control is configured to require that FortiClient AV is enabled and its database is up-to-date.

```
config endpoint-control profile
edit profile1
set feature-enforcement enable
set require-av enable
set require-av-uptodate enable
end
```

To require endpoints to use FortiClient firewall protection - web-based manager

- 1 Go to *UTM Profiles > Endpoint Control > Profile* and open the profile for editing.
- 2 Edit the *FortiClient Firewall* application detection entry.
- 3 In *Action*, select *Block*.
- 4 Select *OK*.

To require endpoints to use FortiClient firewall protection - CLI

```
config endpoint-control profile
edit profile1
set feature-enforcement enable
set require-firewall enable
end
```

To require endpoints to use FortiClient web filtering

This is a CLI-only configuration. In the following example, profile1 is configured to require endpoints to use web filtering.

```
config endpoint-control profile
```

```
edit profile1
    set feature-enforcement enable
    set require-webfilter enable
end
```

To require endpoints to use a licensed FortiClient application

This is a CLI-only configuration. In the following example, profile1 is configured to require endpoints to use a licensed copy of FortiClient Endpoint Security.

```
config endpoint-control profile
    edit profile1
        set feature-enforcement enable
        set require-license enable
    end
```

Optionally, you can set `require-license` to `warn` to warn rather than block users of unlicensed FortiClient software.

Setting the default action for applications

To set the default action for applications - web-based manager

- 1 Go to *UTM Profiles > Endpoint Control > Profile* and open the profile for editing.
- 2 Select the last application detection list entry, *All*, and edit it. Select the *Action* to take for any applications **not** included in this application detection list:
 - **Block** — Endpoints must have only the applications you specify and are denied access if any other applications are installed.
 - **Warn** — Endpoints are warned, but not blocked, if they have any applications other than those included in this application detection list.
 - **Allow or Monitor** — Endpoints can have any application installed, and are denied access only if they have an application for which you created a specific Block rule.
- 3 Select *OK*.

To set the default action for applications - CLI

```
config endpoint-control app-detect rule-list
    edit profile1.list
        set other-application-action allow
    end
```

Adding application detection entries

You need to add an application detection entry for any application that requires a different action than the predefined *All* entry.

To create an application detection entry - web-based manager

- 1 With the endpoint control profile open, select *Create New*.
- 2 Select the application *Category*.
- 3 In *Application*, do one of the following:
 - Select *All*.
 - Select *Specify* and then select the application.

- 4 Select the *Action* and *Condition*, depending on the type of rule you are creating:

Application detection rule	Action	Condition
Application is allowed	Allow	N/A
Application must be installed and running	Block or Warn	Not Running
Application must be installed	Block or Warn	Not Installed
Application must not be running	Block or Warn	Running
Application must not be installed	Block or Warn	Installed
Monitor endpoint with this application running	Monitor	Running
Monitor endpoint with this application installed	Monitor	Installed

The Warn option permits users to connect after viewing a warning.

- 5 Select *OK*.
- 6 To create additional application detection entries, repeat steps 1 through 5.

To create an application detection list - CLI

This example creates an application sensor that denies access to endpoints with peer-to-peer file sharing applications installed. All other applications are allowed.

```
config endpoint-control app-detect rule-list
edit "applist1"
config entries
edit 1
set application 0
set category 15
set vendor 0
set status installed
set action deny
end
set other-application-action allow
end
config endpoint-control profile
edit profile1
set application-detection enable
set application-detection-rule-list profile1.list
end
```

Viewing the application database

You can view the application list provided by FortiGuard Services. Go to *UTM Profiles > Endpoint Control > Application Database*.

Figure 13: Endpoint Control Predefined application list

Category	Name	Vendor	ID	Group
Anti-Malware Software	ActiveSc Application	Null	3077	Security
Anti-Malware Software	Agnitum Outpost Service	Agnitum Ltd.	3078	Security
Anti-Malware Software	Agnitum Outpost	Agnitum Ltd.	3079	Security
Anti-Malware Software	Kingsoft Internet Security	Kingsoft	3080	Security
Anti-Malware Software	SuiMainExe	AhnLab Inc.	3081	Security
Anti-Malware Software	VSCORE.14.1.0.496.x86	McAfee, Inc.	1802	Security
Anti-Malware Software	AhnLab MyKeyDefense 2.5	AhnLab Inc.	3082	Security
Anti-Malware Software	360杀毒	360.CN	1803	Security
Anti-Malware Software	VSCORE.14.1.0.447.x86	McAfee Inc.	3083	Security
Anti-Malware Software	TrendSecure Common Platform	Trend Micro Inc.	1804	Security
Anti-Malware Software	360rpt	360.CN	2316	Security

1 / 61 [Total Applications: 3037] [Column Settings] [Clear All Filters]

The list contains the following information. You can select the name of any column to sort the data by that field. You can also create filters on each column.

Application Database page	
Lists all the applications that are provided by FortiGuard Services	
Column Settings	Select the columns to display in the list. You can also determine the order in which they appear.
Filter Settings	Set and clear column display filters.
Category	The type of application. Example: Document Viewers
Name	The name of the application.
Vendor	The vendor that the application is associated with. For example, the Adobe Reader is associated with the vendor, Adobe Systems Incorporated.
ID	Unique application ID.
Group	Another categorization of the applications. Groups are not used in application sensor rules.
Page controls	Shows the current page number in the list. Select the left and right arrows to display the first, previous, next or last page of known endpoints.
[Total Signatures: <number>]	The total number of application signatures currently in the database.

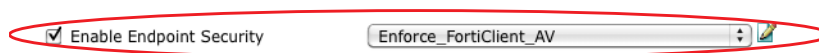
Enabling Endpoint Control in firewall policies

Endpoint Control is applied to any traffic where the controlling firewall policy has Endpoint Security enabled. The selected Endpoint Control profile determines the conditions that govern network access.

You can also enable Endpoint Security in combination with identity-based firewall policies. Users must authenticate and their computers must meet the requirements of the Endpoint Control profile.

To enable Endpoint Control - web-based manager

- 1 Go to *Policy > Policy > Policy* and edit the firewall policy where you want to enable Endpoint Control.
- 2 Select Enable Endpoint Security and select the Endpoint Control profile.

Figure 14: Enabling Endpoint Security in a firewall policy

3 Select OK.

To configure the firewall policy - CLI

In this example, the LAN connects to Port 2 and the Internet is connected to Port 1. An Endpoint Control profile is applied.

```
config firewall policy
  edit 0
    set srcintf port2
    set dstintf port1
    set srcaddr LANusers
    set dstaddr all
    set action accept
    set schedule "always"
    set service "ANY"
    set nat enable
    set endpoint-check enable
    set endpoint-profile "our_profile"
  end
```

Monitoring endpoints

You can view statistical information about the endpoints that were subject to endpoint control. Data is gathered every 15 minutes and the display statistics are for the past 24 hours.

Endpoint status

Endpoint Status displays a pie chart showing the proportions of the endpoint population that:

- do not have FortiClient Endpoint Security installed
- have FortiClient Endpoint Security installed, but do not completely comply with the endpoint profile
- are fully compliant with the endpoint security profile.

To view this display, go to *UTM Profiles > Monitor > Endpoint Monitor* and in *Report by* select *Status*.

You can click on the chart for a detailed list of endpoints.

Figure 15: Endpoint Monitor detailed endpoints list

Refresh Filter Settings Return									
View Compliant									
Compliant	Host Name	IP Address	User	OS Version	FortiClient Version	AV Signature	Detected Applications	CPU Model	System Uptime
✓	DareDevil	192.168.100.125	Administrator	Microsoft Windows XP Professional Service Pack 3 (build 2600)	4.2.3	13.161	<ul style="list-style-type: none"> FortiClient System Tray Controller Messenger Microsoft® Windows® Operating System VMware Tools TPAutoConnect More Applications... 	Intel(R) Xeon(R) CPU S130 @ 2.00GHz	0 day(s) 0 hour(s) 50 minute(s)

Endpoint Application Usage

Endpoint Application Usage displays a bar chart of the top ten applications by traffic volume. The counts include all endpoints with FortiClient Endpoint Security installed that are subject to endpoint control. You can select any of the chart bars to see a list of the top ten endpoints contributing to the data volume for that application.

To view this display, go to *UTM Profiles > Monitor > Endpoint Monitor* and in *Report by* select *Application Usage*.

Endpoint Traffic

Endpoint Traffic displays a bar chart of the top ten endpoints by traffic volume. The counts include all endpoints with FortiClient Endpoint Security installed that are subject to endpoint control. You can select any of the chart bars to see a list of the top ten applications on that endpoint by traffic volume.

To view this display, go to *UTM Profiles > Monitor > Endpoint Monitor* and in *Report by* select *Traffic*.

Modifying Endpoint Security replacement pages

The FortiGate unit sends one of the following HTML pages to a non-compliant user who attempts to use a firewall policy in which Endpoint Security is enabled:

- *Endpoint NAC Block Page* — The endpoint has FortiClient Connect installed, rather than FortiClient Endpoint Security. In the profile's FortiClient application detection entry, the *Block* action is selected. The user should check the FortiClient Connect console to view the exact reason why the endpoint is blocked.
- *Endpoint NAC Recommendation Block Page* — This is the warning version of the *Endpoint NAC Block Page*. The user can select the *Continue to* link to access their desired destination. In the profile's FortiClient application detection entry, the *Warn* action is selected.
- *Endpoint NAC Download Portal* — The endpoint does not have FortiClient Endpoint Security installed. In the profile's FortiClient application detection entry, the *Block* action is selected. The user must install the FortiClient application to proceed. The page includes a download link for the FortiClient installer.

If you modify this replacement message, be sure to retain the `%%LINK%%` tag which provides the download URL for the FortiClient installer.

- *Endpoint NAC Recommendation Portal* — This is the warning version of the *Endpoint NAC Download Portal*. In the profile's FortiClient application detection entry, the *Warn* action is selected. The user can select the *Continue to* link to access their desired destination, without installing FortiClient Endpoint Security. The page also includes a download link for the FortiClient installer.

If you modify this replacement message, be sure to retain both the `%%LINK%%` tag which provides the download URL for the FortiClient installer and the `%%DST_ADDR%%` link that contains the URL that the user requested.

- *Endpoint NAC Feature Block Page* — The endpoint does not have all of the required FortiClient features running. In the profile, the FortiClient feature application detection entry for the missing feature - AV, Firewall, or webfilter (CLI only) - has the *Block* action selected. The message lists the non-compliances. The user must correct the FortiClient settings and try again.

- *Endpoint NAC Recommendation Feature Block Page* — This is the warning version of the *Endpoint NAC Feature Block Page*. In this case, the FortiClient feature application detection entry for the missing feature - AV, Firewall, or webfilter (CLI only) - has the *Warn* action selected. The message lists the non-compliances. The user can select the *Continue* to link to access their desired destination without correcting the non-compliances.

To modify endpoint security replacement messages - web-based manager

- 1 Go to *UTM Profiles > Endpoint Control > Profile* and open the profile for editing.
- 2 Select *Customize Endpoint Messages* and then select the *Edit* icon.
The *Edit Message* window opens.
- 3 In the *Message* box, select the message that you want to modify.
- 4 In the *Message HTML* box, modify the message HTML code.
- 5 Select *OK*.
- 6 Select *OK* to save the changes to the profile.

Example

The Example company has the following requirements for employee computers:

- must run FortiClient Endpoint Security version 4.1.3 with firewall enabled
- must have OpenOffice installed
- cannot have any peer-to-peer file sharing applications installed
- must not have any games running
- all other applications are allowed

Configuring FortiClient download source and required version

FortiGuard Services will provide the FortiClient installer.

To configure FortiClient requirements - web-based manager

- 1 Go to *UTM Profiles > Endpoint Control > Client Installers*.
- 2 Check that *FortiGuard Availability* shows a green checkmark icon.
If you see a red 'X' icon, check your FortiGuard configuration.
- 3 Under *FortiGuard Installer Download Location*, select *FortiGuard Distribution Network*.
- 4 Select *Enforce Minimum Version* and then select 4.1.3 from the list.
- 5 Select *Apply*.

To configure FortiClient requirements - CLI

```
config endpoint-control settings
  set download-location fortiguard
  set version-check minimum
  set version 4.1.3
  set compliance-timeout 5
end
```

Creating an endpoint control profile

The endpoint control rules for FortiClient Endpoint Security and other applications are contained within an endpoint control profile.

To create an endpoint control profile

- 1 Go to *UTM Profiles > Endpoint Control > Profile*.
- 2 Select *Create New*, enter a *Name* for the profile, and then select *OK*.

To create an endpoint control profile

In this example, profile1 is created.

```
config endpoint-control profile
  edit profile1
end
```

Configuring FortiClient application detection entries

The FortiClient application detection entry is configured by default to block endpoints that do not have FortiClient installed and running. The FortiClient AV and FortiClient Firewall entries by default allow endpoints access even if they are not using these features. Only the FortiClient Firewall entry needs to be modified.

To configure the FortiClient Firewall application detection entry

- 1 Go to *UTM Profiles > Endpoint Control > Profile* and open your profile for editing.
- 2 Open the *FortiClient Firewall* entry for editing.
- 3 In *Action*, select *Block*.
- 4 Select *OK*.
- 5 Select *OK* to save the change to your profile.

To configure the FortiClient Firewall application detection entry - CLI

```
config endpoint-control profile
  edit profile1
    set feature-enforcement enable
    set require-firewall enable
  end
```

Configuring application detection entries for other applications

You need to create application detection rules for OpenOffice, P2P applications, and games.

To configure the application sensor - web-based manager

- 1 Go to *UTM Profiles > Endpoint Control > Profile* and open your profile for editing.
- 2 Select *Create New*, enter the following information, and then select *OK*:

This creates a rule requiring the OpenOffice suite.

Category	Office
Application	Specify
Browse	Open Office
Filter by Vendor	Disabled

Action	Block
Condition	Not Installed

- 3 Select *Create New*, enter the following information, and then select *OK*:
This creates a rule denying users with P2P applications installed.

Category	P2P File Sharing
Application	All
Action	Block
Status	Installed

- 4 Select *Create New*, enter the following information, and then select *OK*:
This creates a rule denying users with games applications running.

Category	Games
Application	All
Action	Block
Status	Running

- 5 Select the last application detection list entry, *All*, and edit it. In *Action* select *Allow*.
6 Select *OK*.
7 Select *OK* to save the changes to your profile.

To configure the application detection list and endpoint control profile - CLI

By convention, the application detection entries in the CLI are contained in a rule list prefixed with the profile name. For example, the rule list for profile1 is profile1.list.

The three application detection entries are entered in the same order as for the web-based manager, above. To find codes, use the '?'. For example, `set vendor ?` lists the vendor codes.

```
config endpoint-control app-detect rule-list
edit profile1.list
config entries
edit 1
set application 77
set category 31
set status not-installed
set action deny
next
edit 2
set category 15
set status installed
set action deny
next
edit 3
set category 20
set status running
set action deny
end
set other-application-action allow
end
```

```
config endpoint-control profile
  edit "our_profile"
    set application-detection enable
    set application-detection-rule-list profile1.list
  end
```

Configuring the firewall policy

The firewall policy enables access to the Internet, but requires hosts to meet the Endpoint Control requirements configured in the Endpoint Control profile that you configured earlier.

To configure the firewall policy - web-based manager

- 1 Go to *Policy > Policy* and select *Create New*.
- 2 Enter the following information and select *OK*:

Source Interface/Zone	Select the interface which connects to the LAN.
Source Address	Select the LAN address range.
Destination Interface/Zone	Select the interface which connects to the Internet.
Destination Address	All
Schedule	as required
Service	ANY
Action	ACCEPT
NAT	Enable NAT
Enable Endpoint Security	Select the Endpoint Control profile that you configured earlier.

To configure the firewall policy - CLI

In this example, the LAN connects to Port 2 and the Internet is connected to Port 1.

```
config firewall policy
  edit 0
    set srcintf port2
    set dstintf port1
    set srcaddr LANusers
    set dstaddr all
    set action accept
    set schedule "always"
    set service "ANY"
    set nat enable
    set endpoint-check enable
    set endpoint-profile profile1
  end
```

Endpoint Control interface reference

The Endpoint Control menu helps you to configure profiles, application sensors and databases, including network monitoring.

Endpoint control requires that all hosts using the security policy have the FortiClient Endpoint Security application installed. Make sure that all hosts affected by this policy are able to install this application. Currently, FortiClient Endpoint Security is available for only Microsoft Windows 2000 and later.

To set up endpoint control, you need to:

- Enable Central Management if you are going to use FortiGuard Services to update the FortiClient application or antivirus signatures. You do not need to enter account information.
- Configure the minimum required version of FortiClient and the source of FortiClient installer downloads for non-compliant endpoints. See [“Configuring FortiClient required version and download location” on page 227](#).
- Define application detection lists to specify which applications are allowed or not allowed. Optionally, you can deny access to endpoints that have applications installed that are not on the detection list. See [“FortiGuard” on page 407](#).
- Configure endpoint profiles which specify the FortiClient enforcement settings and the application detection list to apply.
- In firewall policies, enable Endpoint Security and select the Endpoint profile to use.
- Optionally, modify the inactivity timeout for endpoints. The default is 5 minutes. After that time period, the Fortinet unit rechecks the endpoint for Endpoint compliance. To change the timeout, adjust the `compliance-timeout` value in the `config endpoint settings` CLI command.

You can also modify the appearance of the *Endpoint Download Portal* and the *Endpoint Recommendation Portal* by making changes within their replacement messages which are Endpoint Download Portal and Endpoint Recommendation Portal.

This topic includes the following:

- [Profile](#)
- [Application Database](#)
- [Configuring FortiClient required version and download location](#)

Profile

An endpoint control profile contains FortiClient enforcement settings and can specify an application detection list. Security policies can apply an endpoint profile to the traffic they handle.

The following are endpoint profile configuration settings in *UTM Profiles > Endpoint Control > Profile*.

Profile Settings page	
Provides settings for configuring an endpoint control profile. When you edit an existing endpoint profile, you are automatically redirected to this page.	
Name	The name that was entered in the <i>Name</i> field on the New Detection List page. To change the name, edit the text in this field and then select OK.
Comments	The comment that was entered in the <i>Comment</i> field on the New Detection List page. If you want to edit or add a comment, enter the text in this field and then select OK.

Customize Endpoint Messages	Select to allow modifying the Endpoint NAC replacement messages. Select <i>Edit</i> to modify a specific replacement message. When you select <i>Edit</i> , the Edit Message window appears where you can modify each endpoint NAC replacement message.
Create New	Creates a new application entry. When you select <i>Create New</i> , you are automatically redirected to the New Application Detection Entry page.
Edit	Modifies settings within an application entry. When you select <i>Edit</i> , you are automatically redirected to the Edit Application Detection Entry page.
Delete	Removes an entry from within the list. To remove multiple entries from within the list, on the Profile Settings page, in each of the rows of the entries you want removed, select the check box and then select <i>Delete</i> . To remove all entries in the list, on the Profile Settings page, select the check box in the check box column, and then select <i>Delete</i> .
Insert	Inserts a new application detection entry in the list. When you select <i>Insert</i> , you are automatically redirected to the New Application Detection Entry page.
Move To	Moves the entry to another position in the list. When you select <i>Move To</i> , the Move Application Detection Entry window appears. To move an entry, select the new position <i>Before</i> or <i>After</i> , which will place the current entry before or after then entry you enter in the (<i>Entry ID</i>) field. Enter the entry ID number in the field and then select <i>OK</i> .
ID	The identification number for that application detection entry. This number is used when moving an entry within the list.
Application or Category	The category and vendor. If you selected <i>All Applications</i> , then <i>All</i> will appear at the end. For example, Avaya Inc. - Games - All.
Action	The type of action that the unit will take when a match is found.
Condition	The status of the application or category, for example if the FortiClient software is not installed and not running.

New/Edit Application Detection Entry page

You can edit or create a new application detection entry from the UTM Profiles > Endpoint Control > Profile page.

Category	<p>Select the software category for the entry. For example, Instant Messaging.</p> <p>This is not available for the preconfigured FortiClient application detection entries.</p>
Application	<p>Select whether to include all applications in the application detection entry or specify an application. You cannot specify multiple applications per application detection entry.</p> <p>When you select <i>Specify</i>, you can use the <i>Search</i> field to find a specific application or select one from the <i>Browse</i> list. You can also select the check box beside <i>Filter By Vendor</i> to filter the applications by vendor as well.</p>
Tags	<p>You can add tags to an application detection entry. If tag configuration settings are not available, they are disabled on the web-based manager. You must enable them in <i>System > Admin > Settings</i>. See “General Settings” on page 359.</p> <p>To add a tag, enter the tag name in the <i>Add tags</i> field and select the plus sign. To add multiple tags, enter the tags and separate each with a comma and then select the plus sign. The tags that you create are shown in the <i>Applied tags</i> row.</p> <p>This is not available for the preconfigured FortiClient entries.</p>
Action	<p>Select what to do if the application is running on the endpoint:</p> <ul style="list-style-type: none"> • <i>Allow</i> – allows the endpoint to connect • <i>Block</i> – quarantines the endpoint • <i>Monitor</i> – includes this endpoint’s information in statistics and logs on the Endpoint Monitor page. • <i>Warn</i> – displays a block page, but contains a button to let the user continue at his or her discretion. Information is then sent back to the client.
Condition	<p>Select the status of the application.</p> <ul style="list-style-type: none"> • <i>Installed</i> – application is installed but no currently running. • <i>Running</i> – application is currently running • <i>Not Installed</i> – application is not currently installed • <i>Not Running</i> – application is not currently running

Application Database

The Application Database page allows you to view the applications which are sorted by category. For example, iKey is found under the Encryption PKI category. This page also allows you to apply tags the applications within the list, search to find a particular application or category, as well as filter the applications within the list.

Lists the applications. On this page, you can create tags for applications, search, as well as filter and customize columns.

Tags	<p>Adds or removes tags to the applications in the application database list. If tag configuration settings are not available, they are disabled on the web-based manager. You must enable them in <i>System > Admin > Settings</i>. See “Tag management” on page 582.</p> <p>When you select the down arrow beside Tags, you can add or removed tags.</p> <p>To add tags to an application in the list, select the application first and then select the down arrow beside <i>Tags</i> to select <i>Add Tags</i>. The Add Tags window appears. Enter the tag in the <i>Add tag</i> field and select the plus sign to add the tag <i>Tags</i> to apply. Select <i>OK</i> to permanently add the tags to the application.</p> <p>To remove a tag in application in the list, select the application first and then select the down arrow beside <i>Tags</i> to select <i>Remove Tags</i>. Select the tag in the <i>Applied tags</i> row; it automatically moves to the <i>Tags to remove</i> row. Repeat until all tags are listed in the <i>Tags to remove</i> row. Select <i>OK</i> to permanently remove the tags from the application.</p> <p>If there are tags that you want to add to an application that have been configured for another object, such as an application within <i>UTM Profiles > Application Control > Application List</i>, you can add those tags as well to the application in the application database.</p> <p>To apply these other object tags, select the application and then select the down arrow beside <i>Tags</i>; select <i>Add Tags</i>. In the <i>Add Tags</i> window, select each of the tags you want to add from within the <i>Click tag to add</i> row. Each tag is automatically added to the <i>Tags to apply</i> row. Select <i>OK</i> to add them to the application in the application database.</p>
Column Settings	<p>Customize the column view. You can select the columns to hide or display them and specify the column display order.</p>

Filter Settings	<p>Select to filter the information on the Application Database page. Filters appears automatically after selecting <i>Filter Settings</i>, below the column headings.</p> <p>Note: <i>Filter Settings</i> configures all filter settings. Filter icons are used to configure filter settings within that column.</p> <p>To apply a filter setting, select the plus sign beside <i>Add new filter</i> and then select and enter the information required. Repeat to add other filter settings.</p> <p>To modify settings, select <i>Change</i> beside the setting and edit the settings.</p> <p>To clear all filter settings, select the icon beside <i>Clear all filters</i>.</p> <p>To use a filter icon to filter settings within a column, select the filter icon in the column; <i>Filters</i> appears. Within <i>Filters</i>, configure the filter settings for that column.</p> <p>The <i>Filter Settings</i> on the Application Database page contains the option <i>Copy to Profile</i>, which allows you to copy the filter settings and apply them to an endpoint profile.</p> <p>To apply existing filter settings to an endpoint profile, select the down arrow beside <i>Filter Settings</i> and then select <i>Copy to Profile</i>. In the <i>Select Object window</i>, select the endpoint profile from the <i>Endpoint Profile's</i> drop-down list. Select <i>OK</i>.</p>
Search	<p>Enter a search criteria into the field and then press Enter on your keyboard. Use the <i>Clear All</i> icon beside the field to clear the search results.</p>
Category	<p>The type of category an application is included in. For example, Anti-Mailware Software includes the Billy The Goat application.</p> <p>This column can display the application database list information in ascending or descending order. Select the green arrow beside Category; a green down arrow means the information is in descending order and an green up arrow means the information is in ascending order.</p>
Name	The name of the application.
Vendor	The name of the vendor.
Tags	The tag or tags that were created for the application.
Page Controls	Use to navigate through the list.
[Total Applications:]	The maximum number of applications that are currently shown in the list on the Application Database page.

Client Installers

You can set the minimum FortiClient version that endpoints are required to run from *UTM Profiles > Endpoint Control > Client Installers*. The FortiClient Endpoint Security page also configures the download source for the FortiClient installer.

Information section	
Indicates the FortiGuard availability and current versions of antivirus and application signatures packages. This section also allows you to update your antivirus and application signature packages, as well as downloading a Windows Installer.	
FortiGuard Availability	FortiGuard Services is available if the indicator is green.
FortiClient Endpoint Versions	FortiClient software versions available from FortiGuard Services are listed. Select the <i>Download</i> link to download the installer for either a Mac computer or Windows computer.
AV Signature Package	The latest AV signature package available from FortiGuard Services.
Application Signature Package	The latest application signature package available from FortiGuard Services.
FortiClient Downloads	The number of FortiClient software downloads through this Fortinet unit.
Update Now	Retrieve the latest information from FortiGuard Services.
FortiClient Installer Download Location section	
Select one of the following options to determine the link that the FortiClient Download Portal provides to non-compliant users to download the FortiClient installer.	
FortiGuard Distribution Network	<p>The FortiClient application is provided by the FortiGuard Distribution Network. The Fortinet unit must be able to access the FortiGuard Distribution Network.</p> <p>If the Fortinet unit contains a hard disk drive, the files from FortiGuard Services are cached to more efficiently serve downloads to multiple end points.</p>
This Fortinet	<p>Users download a FortiClient installer file from this unit.</p> <p>This option is available only on FortiGate models that support upload of FortiClient installer files. Upload your FortiClient installer file using the <code>execute restore forticlient</code> CLI command. For more information, refer to the FortiGate CLI Reference.</p>
Custom URL	Specify a URL from which users can download the FortiClient installer. You can use this option to provide custom installer files even if your unit does not have storage space for them.

FortiClient Version section	
Enforce Minimum Version ... (If enabled in Endpoint Profiles)	<p>From the list select either <i>Latest Available</i> or a specific FortiClient version as the minimum requirement for endpoints.</p> <p>The list contains the FortiClient versions available from the selected <i>FortiClient Installer Download Location</i>.</p> <p>Fortinet recommends that administrators deploy a FortiClient version update to their users or ask users to install the update and then wait a reasonable period of time for the updates to be installed before updating the minimum version required to the most recent version.</p>



Select *Custom URL* if you want to provide a customized FortiClient application. This is required if a FortiManager unit will centrally manage FortiClient applications. For information about customizing the FortiClient application, see the [FortiClient Administration Guide](#).



Vulnerability Scan

The Network Vulnerability Scan helps you to protect your network assets (servers and workstations) by scanning them for security weaknesses. You can scan on-demand or on a scheduled basis. Results are viewable on the FortiGate unit, but results are also sent to an attached FortiAnalyzer unit. The FortiAnalyzer unit can collect the results of vulnerability scans from multiple FortiGate units at different locations on your network, compiling a comprehensive report about network security.

This section describes how to configure a single FortiGate unit for network scanning and how to view the results of the scan.

The following topics are included in this section:

- [Overview](#)
- [Selecting assets to scan](#)
- [Configuring scans](#)
- [Viewing scan results](#)

Overview

Network vulnerability scanning has three main parts:

- Select the assets to scan
- Schedule scans or initiate them manually
- View the scan results

Selecting assets to scan

An asset is a server or workstation computer on your network. You can specify assets individually, but it is easier to use the network vulnerability scan feature's asset discovery function. The discovery function searches a specified IP address range and populates the asset list. You then select the assets to include in network vulnerability scans.

Asset discovery scans the following ports:

- TCP: 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445
- UDP: 53, 111, 135, 137, 161, 500

Discovering assets

The simplest way to build the Asset list is to perform a discovery scan on the range of IP addresses where your network assets are installed.

To discover assets - web-based manager

- 1 Go to *UTM Profiles > Vulnerability Scan > Asset Definition* and select *Create New*.
- 2 Enter a *Name* for this scan.
- 3 In *Type*, select *Range* and then enter the IP address *Range* to scan.

4 Select *OK*.

This creates an entry in the Asset list.

5 Select the asset list entry that you just created and then select *Discover Assets*.

Above the table header, on the top right, the status of the current scan is shown. Depending on the number of computers to be discovered, the scan can take several minutes, until the web-based manager reports "Scan completed." The number of assets discovered is listed to the left of the *Discover Assets* button.

6 Select *Assets Found* and then select *Import*.

The discovered assets are added to the Asset list. By default, all are enabled for scanning.

7 Unless you want to discover assets on every scan, clear the Enable check box for this Asset discovery only asset.

You might want to add authentication credentials to some of your assets. To edit an entry in the Asset list, select its check box (at the left side of the list) and then select *Edit*. For more information about individual asset settings, see ["Adding assets manually"](#), below.

To discover assets - CLI

This example discovers assets in the range 10.11.101.10 to 10.11.101.200.

1 First configure the asset range to scan:

```
config netscan assets
  edit 0
    set name "office_discovery"
    set addr-type range
    set start-ip 10.11.101.10
    set end-ip 10.11.101.200
    set mode discovery
    set status enable
  end
```

2 Execute the discovery scan:

```
execute netscan start discover
```

3 Check the status of the discovery scan:

```
execute netscan status
```

Repeat periodically until status is "scan complete".

4 Optionally, view a list of the discovered assets:

```
execute netscan list
```

5 Add the discovered assets to the asset list:

```
execute netscan import
```

Adding assets manually

There is no need to perform a discovery scan if you know the IP address of the computer that you want to scan, or you know that you want to scan all of the computers in a particular IP address range.

If you create an asset with an IP address range, any authentication credentials you enter will apply to all devices in the range. If this is not appropriate, you need to create individual entries for each computer instead.

To add an asset - web-based manager

- 1 Go to *UTM Profiles > Vulnerability Scan > Asset Definition* and select *Create New*.
- 2 Enter the following information and select *OK*:

Name	Enter a name for this asset.
Type	Select <i>Host</i> to configure a single IP address. Select <i>Range</i> to configure a range of IP addresses to scan.
IP Address	Enter the IP address of the asset. (<i>Type is Host.</i>)
Range	Enter the start and end of the IP address range. (<i>Type is Range.</i>)
Scan Type	Select <i>Vulnerability Scan</i> .
Windows Authentication	Select to use authentication on a Windows operating system. Enter the username and password in the fields provided. For more information, see “Requirements for authenticated scanning” on page 252 .
Unix Authentication	Select to use authentication on a Unix operating system. Enter the username and password in the fields provided. For more information, see “Requirements for authenticated scanning” on page 252 .

To add an asset - CLI

This example adds a single computer to the Asset list:

```
config netscan assets
edit 0
    set name "server1"
    set addr-type ip
    set start-ip 10.11.101.20
    set mode scan
    set auth-windows enable
    set win-username admin
    set win-password zxcvbnm
    set status enable
end
```

This example adds an address range to the Asset list. Authentication is not used:

```
config netscan assets
edit 0
    set name "fileservers"
    set addr-type range
    set start-ip 10.11.101.160
    set end-ip 10.11.101.170
    set mode scan
    set status enable
end
```

Requirements for authenticated scanning

The effectiveness of an authenticated scan is determined by the level of access the FortiGate unit obtains to the host operating system. Rather than use the system administrator's account, it might be more convenient to set up a separate account for the exclusive use of the vulnerability scanner with a password that does not change.

Microsoft Windows hosts - domain scanning

The user account provided for authentication must

- have administrator rights
- be a Security type of account
- have global scope
- belong to the Domain Administrators group
- meet the Group Policy requirements listed below:

Group Policy - Security Options

In the Group Policy Management Editor, go to Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.

Setting	Value
Network access: Sharing and security model for local accounts	Classic
Accounts: Guest account status	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled

Group Policy - System Services

In the Group Policy Management Editor, go to Computer Configuration > Windows Settings > Security Settings > System Services.

Setting	Value
Remote registry	Automatic
Server	Automatic
Windows Firewall	Automatic

Group Policy - Administrative Templates

In the Group Policy Management Editor, go to Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile.

Setting	Value
Windows Firewall: Protect all network connections	Disabled

or

Setting	Value
Windows Firewall: Protect all network connections	Enabled
Windows Firewall: Allow remote administration exception Allow unsolicited messages from ¹	Enabled *
Windows Firewall: Allow file and printer sharing exception	Enabled

Allow unsolicited messages from ¹	*
Windows Firewall: Allow ICMP exceptions	Enabled
Allow unsolicited messages from ¹	*

¹Windows prompts you for a range of IP addresses. Enter either "*" or the IP address of the Fortinet appliance that is performing the vulnerability scan.

Microsoft Windows hosts - local (non-domain) scanning

The user account provided for authentication must

- be a local account
- belong to the Administrators group

The host must also meet the following requirements:

- Server service must be enabled. (Windows 2000, 2003, XP)
- Remote Registry Service must be enabled.
- File Sharing must be enabled.
- Public folder sharing must be disabled. (Windows 7)
- Simple File Sharing (SFS) must be disabled. (Windows XP)

Windows firewall settings

- Enable the *Remote Administration Exception* in Windows Firewall. (Windows 2003, Windows XP)
- Allow *File and Print sharing* and *Remote Administration* traffic to pass through the firewall. Specify the IP address or subnet of the Fortinet appliance that is performing the vulnerability scan. (Windows Vista, 2008)
- For each of the active *Inbound Rules* in the *File and Printer Sharing* group, set the *Remote IP address* under *Scope* to either *Any IP address* or to the IP address or subnet of the Fortinet appliance that is performing the vulnerability scan. (Windows 7)

Unix hosts

The user account provided for authentication must be able at a minimum to execute these commands:

- The account must be able to execute "uname" in order to detect the platform for packages.
- If the target is running Red Hat, the account must be able to read /etc/redhat-release and execute "rpm".
- If the target is running Debian, the account must be able to read /etc/debian-version and execute "dpkg".

Configuring scans

You can configure regular network scans on a daily, weekly, or monthly basis. There are three scan modes. Full scan checks every TCP and UDP port and takes the most time. Standard scan checks the ports used by most known applications. Quick scan checks only the most commonly used ports. For a detailed list of the TCP and UDP ports examined by each scan mode, see [Table 15 on page 255](#). Also, the `get netscan settings` CLI command lists the TCP and UDP ports scanned in the current scan mode. See the `tcp-ports` and `udp-ports` fields.

You can also initiate the configured scan manually.

Table 15: Ports scanned in each scan mode

Standard Scan	<p>TCP: 1-3, 5, 7, 9, 11, 13, 15, 17-25, 27, 29, 31, 33, 35, 37-39, 41-223, 242-246, 256-265, 280-282, 309, 311, 318, 322-325, 344-351, 363, 369-581, 587, 592-593, 598, 600, 606-620, 624, 627, 631, 633-637, 666-674, 700, 704-705, 707, 709-711, 729-731, 740-742, 744, 747-754, 758-765, 767, 769-777, 780-783, 786, 799-801, 860, 873, 886-888, 900-901, 911, 950, 954-955, 990-993, 995-1001, 1008, 1010-1011, 1015, 1023-1100, 1109-1112, 1114, 1123, 1155, 1167, 1170, 1207, 1212, 1214, 1220-1222, 1234-1236, 1241, 1243, 1245, 1248, 1269, 1313-1314, 1337, 1344-1625, 1636-1774, 1776-1815, 1818-1824, 1901-1909, 1911-1920, 1944-1951, 1973, 1981, 1985-2028, 2030, 2032-2036, 2038, 2040-2049, 2053, 2065, 2067, 2080, 2097, 2100, 2102-2107, 2109, 2111, 2115, 2120, 2140, 2160-2161, 2201-2202, 2213, 2221-2223, 2232-2239, 2241, 2260, 2279-2288, 2297, 2301, 2307, 2334, 2339, 2345, 2381, 2389, 2391, 2393-2394, 2399, 2401, 2433, 2447, 2500-2501, 2532, 2544, 2564-2565, 2583, 2592, 2600-2605, 2626-2627, 2638-2639, 2690, 2700, 2716, 2766, 2784-2789, 2801, 2908-2912, 2953-2954, 2998, 3000-3002, 3006-3007, 3010-3011, 3020, 3047-3049, 3080, 3127-3128, 3141-3145, 3180-3181, 3205, 3232, 3260, 3264, 3267-3269, 3279, 3306, 3322-3325, 3333, 3340, 3351-3352, 3355, 3372, 3389, 3421, 3454-3457, 3689-3690, 3700, 3791, 3900, 3984-3986, 4000-4002, 4008-4009, 4080, 4092, 4100, 4103, 4105, 4107, 4132-4134, 4144, 4242, 4321, 4333, 4343, 4443-4454, 4500-4501, 4567, 4590, 4626, 4651, 4660-4663, 4672, 4899, 4903, 4950, 5000-5005, 5009-5011, 5020-5021, 5031, 5050, 5053, 5080, 5100-5101, 5145, 5150, 5190-5193, 5222, 5236, 5300-5305, 5321, 5400-5402, 5432, 5510, 5520-5521, 5530, 5540, 5550, 5554-5558, 5569, 5599-5601, 5631-5632, 5634, 5678-5679, 5713-5717, 5729, 5742, 5745, 5755, 5757, 5766-5767, 5800-5802, 5900-5902, 5977-5979, 5997-6053, 6080, 6103, 6110-6112, 6123, 6129, 6141-6149, 6253, 6346, 6387, 6389, 6400, 6455-6456, 6499-6500, 6515, 6558, 6588, 6660-6670, 6672-6673, 6699, 6767, 6771, 6776, 6831, 6883, 6912, 6939, 6969-6970, 7000-7021, 7070, 7080, 7099-7100, 7121, 7161, 7174, 7200-7201, 7300-7301, 7306-7308, 7395, 7426-7431, 7491, 7511, 7777-7778, 7781, 7789, 7895, 7938, 7999-8020, 8023, 8032, 8039, 8080-8082, 8090, 8100, 8181, 8192, 8200, 8383, 8403, 8443, 8450, 8484, 8732, 8765, 8886-8894, 8910, 9000-9001, 9005, 9043, 9080, 9090, 9098-9100, 9400, 9443, 9535, 9872-9876, 9878, 9889, 9989-10000, 10005, 10007, 10080-10082, 10101, 10520, 10607, 10666, 11000, 11004, 11223, 12076, 12223, 12345-12346, 12361-12362, 12456, 12468-12469, 12631, 12701, 12753, 13000, 13333, 14237-14238, 15858, 16384, 16660, 16959, 16969, 17007, 17300, 18000, 18181-18186, 18190-18192, 18194, 18209-18210, 18231-18232, 18264, 19541, 20000-20001, 20011, 20034, 20200, 20203, 20331, 21544, 21554, 21845-21849, 22222, 22273, 22289, 22305, 22321, 22555, 22800, 22951, 23456, 23476-23477, 25000-25009, 25252, 25793, 25867, 26000, 26208, 26274, 27000-27009, 27374, 27665, 29369, 29891, 30029, 30100-30102, 30129, 30303, 30999, 31336-31337, 31339, 31554, 31666, 31785, 31787-31788, 32000, 32768-32790, 33333, 33567-33568, 33911, 34324, 37651, 40412, 40421-40423, 42424, 44337, 47557, 47806, 47808, 49400, 50505, 50766, 51102, 51107, 51112, 53001, 54321, 57341, 60008, 61439, 61466, 65000, 65301, 65512</p> <p>UDP: 7, 9, 13, 17, 19, 21, 37, 53, 67-69, 98, 111, 121, 123, 135, 137-138, 161, 177, 371, 389, 407, 445, 456, 464, 500, 512, 514, 517-518, 520, 555, 635, 666, 858, 1001, 1010-1011, 1015, 1024-1049, 1051-1055, 1170, 1243, 1245, 1434, 1492, 1600, 1604, 1645, 1701, 1807, 1812, 1900, 1978, 1981, 1999, 2001-2002, 2023, 2049, 2115, 2140, 2801, 3024, 3129, 3150, 3283, 3527, 3700, 3801, 4000, 4092, 4156, 4569, 4590, 4781, 5000-5001, 5036, 5060, 5321, 5400-5402, 5503, 5569, 5632, 5742, 6073, 6502, 6670, 6771, 6912, 6969, 7000, 7300-7301, 7306-7308, 7778, 7789, 7938, 9872-9875, 9989, 10067, 10167, 11000, 11223, 12223, 12345-12346, 12361-12362, 15253, 15345, 16969, 20001, 20034, 21544, 22222, 23456, 26274, 27444, 30029, 31335, 31337-31339, 31666, 31785, 31789, 31791-31792, 32771, 33333, 34324, 40412, 40421-40423, 40426, 47262, 50505, 50766, 51100-51101, 51109, 53001, 61466, 65000</p>
----------------------	---

Full Scan	All TCP and UDP ports (1-65535)
Quick Scan	<p>TCP: 11, 13, 15, 17, 19-23, 25, 37, 42, 53, 66, 69-70, 79-81, 88, 98, 109-111, 113, 118-119, 123, 135, 139, 143, 220, 256-259, 264, 371, 389, 411, 443, 445, 464-465, 512-515, 523-524, 540, 548, 554, 563, 580, 593, 636, 749-751, 873, 900-901, 990, 992-993, 995, 1080, 1114, 1214, 1234, 1352, 1433, 1494, 1508, 1521, 1720, 1723, 1755, 1801, 2000-2001, 2003, 2049, 2301, 2401, 2447, 2690, 2766, 3128, 3268-3269, 3306, 3372, 3389, 4100, 4443-4444, 4661-4662, 5000, 5432, 5555-5556, 5631-5632, 5634, 5800-5802, 5900-5901, 6000, 6112, 6346, 6387, 6666-6667, 6699, 7007, 7100, 7161, 7777-7778, 8000-8001, 8010, 8080-8081, 8100, 8888, 8910, 9100, 10000, 12345-12346, 20034, 21554, 32000, 32768-32790</p> <p>UDP: 7, 13, 17, 19, 37, 53, 67-69, 111, 123, 135, 137, 161, 177, 407, 464, 500, 517-518, 520, 1434, 1645, 1701, 1812, 2049, 3527, 4569, 4665, 5036, 5060, 5632, 6502, 7778, 15345</p>

To configure scanning - web-based manager

- 1 Go to *UTM Profiles > Vulnerability Scan > Scan*.
- 2 Enter the following information and select *Apply*.

Scan Mode	<p>Quick — check only the most commonly used ports</p> <p>Standard — check the ports used by most known applications</p> <p>Full — check all TCP and UDP ports</p> <p>For a detailed list of the TCP and UDP ports examined by each scan mode, see Table 15 on page 255.</p>
Schedule	<p>Manually – perform scan on request only</p> <p>Schedule – use the following fields to configure a schedule</p>
Recurrence	<p>Select <i>Daily</i>, <i>Weekly</i>, or <i>Monthly</i>.</p> <p>If you select <i>Weekly</i>, the Day of Week drop-down list appears. If you select <i>Monthly</i>, the Day of Month drop-down list appears.</p>
Time	Select the time of day to start the scan, in the format HH:MM.
Day of Week	For a weekly scan, select the day of the week.
Day of Month	For a monthly scan, select the day of the month.

To configure scanning - CLI

To configure, for example, a standard scan to be performed every Sunday at 2:00am, you would enter:

```
config netscan settings
  set scan-mode standard
  set schedule enable
  set time 02:00
  set recurrence weekly
  set day-of-week sunday
end
```

To perform a vulnerability scan manually - web-based manager

- 1 Go to *UTM Profiles > Vulnerability Scan > Asset*.

- 2 Select the Enable check box for each asset you want to scan.
- 3 Select *Start Scan*.

Above the table header, on the top right, the status of the current scan is shown.

Depending on the number of computers to be discovered, the scan can take several minutes, until the web-based manager reports “Scan completed.”

To perform a vulnerability scan manually - CLI

You must have some assets configured with `mode` set to `scan`.

- 1 Execute the discovery scan:
- 2 Check the status of the discovery scan:

```
execute netscan start scan
```

```
execute netscan status
```

Repeat periodically until status is “scan complete”.

Viewing scan results

The results of network scanning are available as summary graphs and log entries.

Viewing scan logs

To view network scan logs, go to *Log&Report > Log & Archive Access > Vulnerability Scan Log*.

Figure 16: Network scan logs

Refresh Clear All Filters Column Settings Disk Memory HA Cluster: FG600B3908600705 Formatted Raw						
64	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	SSH Server type and version
65	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	Apache mod_proxy_ftp 2.0.x/2.2.x Denial of Service Vuln
66	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	Apache mod_proxy_ftp FTP Command Injection Vulnerab
67	2010-06-01 10:13:45	notice	vulnerability	4090	10.11.101.20	Apache "mod_proxy" Remote Denial of Service Vulnerabi
68	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	Apache OS Fingerprinting Unspecified Security Vulnerabi
69	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	Apache mod_proxy_ftp Wildcard Characters Cross-Site S
70	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	Apache 2.2 Multiple Vulnerabilities
71	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	Determines if we can use the remote web proxy
72	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	This plugin fingerprints the remote web server
73	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	This plugin performs a quick web mirror on the remote w
74	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	http TRACE XSS attack
75	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	HTTP Server type and Version
76	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	Solaris rpc.statd rpc Call Relaying Vulnerability
77	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	Checks for SMB Service on Port 445 and 139
78	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	Check NULL session.
79	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	Checks for SMB Service on Port 445 and 139
80	2010-06-01 10:13:45	notice	vulnerability	4098	10.11.101.20	Gets the port of the remote rpc portmapper
81	2010-06-01 10:13:45	notice	discovery	4100	10.11.101.20	
82	2010-06-01 10:13:45	notice	discovery	4100	10.11.101.20	
83	2010-06-01 10:13:45	notice	discovery	4100	10.11.101.20	
84	2010-06-01 10:13:45	notice	discovery	4100	10.11.101.20	
85	2010-06-01 10:13:45	notice	discovery	4100	10.11.101.20	
86	2010-06-01 10:13:45	notice	discovery	4100	10.11.101.20	
87	2010-06-01 10:13:45	notice	discovery	4100	10.11.101.20	
88	2010-06-01 10:13:45	notice	discovery	4100	10.11.101.20	
89	2010-06-01 10:13:45	notice	discovery	4100	10.11.101.20	
90	2010-06-01 10:13:45	notice	discovery	4100	10.11.101.20	
91	2010-06-01 10:13:45	notice	discovery	4099	10.11.101.20	Linux 2.6.17 - 2.6.27
92	2010-06-01 10:12:16	notice	vulnerability	4096		
93	2010-06-01 10:12:16	notice	vulnerability	4098	10.11.101.20	SSH Server type and version
94	2010-06-01 10:12:16	notice	vulnerability	4098	10.11.101.20	Apache mod_proxy_ftp 2.0.x/2.2.x Denial of Service Vuln

Select any log entry to view log details.

Figure 17: Network scan log details

The screenshot shows the FortiGate Log & Report interface. On the left, a list of log entries is displayed with columns for ID, Date, Time, Notice, Vulnerability, ID, IP Address, and Service. Entry 65 is highlighted. On the right, the 'Log Details' window is open for entry 65, showing the following information:

Date	2010-06-01
Time	10:13:45
Level	notice
Sub Type	vulnerability
ID	4098
Virtual Domain	root
Action	vuln-detection
IP Address	10.11.101.20
Protocol	tcp
Port	80
Vulnerability	Apache mod_proxy_ftp 2.0.x/2.2.x Denial of Service Vulnerability
Vuln Category	web server
Vuln ID	18412
Reference	N/A
Severity	high

Viewing Executive Summary graphs

To view summary graphs, go to *Log&Report > Report Access > Executive Summary*. You might need to add the following widgets to the page to view the summaries you require.

Table 16: Executive summary widgets for network scan

Chart	Widget name
Vulnerabilities by Category	vulner-by-category-last24h
Vulnerabilities by Severity	vulner-by-severity-last24h
Top Vulnerable Operating Systems Detected	top-vulner-os-last24h
Top Vulnerable Services Detected	top-vulner-service-last24h
Top Vulnerable TCP Services Detected	top-vulner-tcp-service-last24h
Top Vulnerable UDP Services Detected	top-vulner-udp-service-last24h

Creating reports

You can use the FortiGate unit's Log&Report features to generate reports on the results of network vulnerability scanning.

To create a report of scanning results

- 1 Go to *Log&Report > Report Config > Layout* and select *Create New*.
- 2 Enter a *Name* for the report.

- 3 Optionally select a *Report Theme*.
- 4 Enter a *Title* to appear on the report.
- 5 Choose each *Option* and *Output Format* that you require.
- 6 If you want to have the report generated on a regular basis, create a *Schedule*.
- 7 Select the *Report Components*.

The components are listed in order below the Report Components heading. For a network vulnerability scan report, you will need to select Chart components from the Vulnerability category. The following vulnerability charts are available:

Table 17: Executive summary widgets for network scan

Chart	Component name
Vulnerabilities by Category	vulner-by-category-last24h
Vulnerabilities by Severity	vulner-by-severity-last24h
Top Vulnerable Operating Systems Detected	top-vulner-os-last24h
Top Vulnerable Services Detected	top-vulner-service-last24h
Top Vulnerable TCP Services Detected	top-vulner-tcp-service-last24h
Top Vulnerable UDP Services Detected	top-vulner-udp-service-last24h

- 8 Optionally select other components, such as headings and text.
- 9 Select OK.

The report will be generated at the scheduled time.

To generate a report manually

- 1 Go to *Log&Report > Report Config > Layout*.
- 2 Select the required report.
- 3 Select *Run*.

Viewing reports

Go to *Log&Report > Report Access > Disk* to view generated reports.

Figure 18: List of reports

Delete					
<input type="checkbox"/>	Report File	Started	Finished	Size (bytes)	Other Formats
<input checked="" type="checkbox"/>	On-Demand-netscanreport-2010-05-03-101952	2010-05-03 10:19:52	2010-05-03 10:19:53	10380	PDF(9.1k)

If HTML output was enabled, you can select the Report File name to view the report in a separate browser window.

If PDF output was enabled, you can select the link in the Other Formats column to view the report.

Vulnerability Scan interface reference

The *Vulnerability Scan* menu enables you to configure scanning of your network, a feature similar to the vulnerability scan features on FortiAnalyzer or FortiScan units.

This topic includes the following:

- [Selecting assets to scan](#)
- [Configuring scans](#)
- [Vulnerability Result](#)

Asset Definition

In the Asset Definition menu, you can configure multiple asset lists that are used for scanning purposes. On the Asset Definition page, you can use an asset list to discover assets, start a scan or view the discovered assets.

The following are asset definition configuration settings in *UTM Profiles > Vulnerability Scan > Asset Definition*.

Asset Definition page	
Lists each individual asset that you created. On this page, you can edit, delete or create a new asset.	
Create New	Creates a new asset. When you select <i>Create New</i> , you are automatically redirected to the Asset Settings page.
Edit	Modifies an asset. When you select <i>Edit</i> , you are automatically redirected to the Asset Settings page.
Delete	Removes an asset from the list on the page.
View	Displays discovered hosts that were found during the scanning process. When you select <i>View</i> , the Discovered Hosts window appears. Select <i>Return</i> to go back to the Asset Definition page.
Discover Assets	Scans to discover assets. When you select <i>Discover Assets</i> , the options <i>Pause</i> and <i>Stop</i> appear. Select <i>Pause</i> to pause the scanning process or select <i>Stop</i> to stop the scanning process altogether.
Start Scan	Starts the scanning process. When you start scanning, the <i>Pause</i> and <i>Stop</i> options appear. Select <i>Pause</i> to pause the scanning process or select <i>Stop</i> to stop the scanning process altogether.
Name	The name of the asset.
IP Address/Range	If <i>Host</i> was chosen as the type for the asset, then the IP address of the host displays. If <i>Range</i> was chosen as the type for the asset, the IP address range appears.
Scheduled Vulnerability Scan	Indicates that there is a scheduled scan.
# Assets Discovered	Indicates how many assets were discovered during the scanning process.
Scan Activity	Indicates the activity of the scan.
Asset Settings page	
Provides settings for configuring an asset.	
Name	Enter a name for the asset that you are creating.
Type	Select <i>Host</i> to configure the host's IP address. Select <i>Range</i> to configure the IP address range.

IP Address (Range)	Enter the IP address of the host, or the IP address range. This depends on what type you selected in <i>Type</i> . If you select <i>Range</i> in <i>Type</i> , then the name <i>Range</i> appears and there are two IP address fields for you to enter the IP address range in.
Enable Scheduled Vulnerability Scanning	Select to schedule a scan.
Windows Authentication	Select to use authentication on a Windows operating system. Enter the username and password in the fields provided. The fields appear after selecting <i>Windows Authentication</i> .
Unix Authentication	Select to use authentication on a Unix operating system. Enter the username and password in the fields provided. The fields appear after selecting <i>Unix Authentication</i> .

Scan Schedule

From the Scan Schedule page, you can view the status of a vulnerability scan, and adjust the times and type of future scans.

The following are configuration settings for scheduling scans in *UTM Profiles > Vulnerability Scan > Scan Schedule*.

Status section	
Indicates the status of the previous scan, as well as when the next scan will occur. You can also start a scan using <i>Start Scan</i> .	
Scan Status	Indicates if a scan is currently running. If you select <i>Start Scan</i> , a scan will immediately begin. A progress bar appears, along with <i>Pause</i> and <i>Stop</i> , and the start time, estimated rating and completion time period. Select <i>Pause</i> to pause the scan or <i>Stop</i> to stop the scan altogether.
Last Scan Start Time	Indicates the last previous scan's start time. The format is <month> <day>, <year> - <hour>:<minute> <AM/PM>. For example, October 12, 2010 - 04:30 PM. The time is in 24-hour format.
Last Scan End Time	Indicates the last previous scan's end time. The format is <month> <day>, <year> - <hour>:<minute> <AM/PM>. For example, October 12, 2010 - 06:30 PM. The time is in 24-hour format.
Last Scan Duration	Indicates how long the scan lasted, in seconds.
Next Scheduled Scan	Indicates when the next scheduled scan will begin.

Schedule section	
Configure the time and day (or date if you choose to schedule a scan on a monthly basis) as well as enable to suspend a scan between a specified time period.	
Recurrence	<p>Select when the schedule should occur, such as on a daily basis or monthly basis.</p> <p>If you select <i>Weekly</i>, you must select the day of the week that the scan will occur on, as well as the hour and minutes.</p> <p>If you select <i>Monthly</i>, you must select the day within the current month as well as the hour and minutes. For example, in the current month of October, <i>Recurrence</i> is set to <i>Monthly</i>, with <i>Day of Month</i> being 20 and <i>Hour</i> being 12, and <i>Minutes</i> being 00.</p>
Suspend Scan between	Select to suspend the unit from scanning the network during a specified time period. Specify the hours and minutes using the drop-down lists.
Vulnerability Scan Mode section	
Select a mode that will be used when scanning network activity.	
Quick	Examines the most commonly used ports for vulnerabilities.
Standard	Examines a large number of application ports which cover many known applications.
Full	Examines the full port range, 1-65535, looking for applications that are running on non-standard ports.
Advanced section	
Provides options for specifying scanning only TCP or UDP ports, as well as operating systems or services.	
Enable TCP Port Scan	Select to scan only TCP ports.
Enable Service Detection	Select to scan for the detection of services on ports.
Enable OS Detection	Select to scan for the detection of operating systems on ports.
Enable UDP Port Scan	Select to scan only UDP ports.

Vulnerability Result

The Vulnerability Scan Results page provides a graphical and tabular representation of the information the FortiGate unit gathered from scanning the network.

The Summary table lists recent scans.

The two bar graphs, *Vulnerabilities by Severity* and *Vulnerabilities by Category* show the number of vulnerabilities that were found by severity and by category.



Sniffer policy

Sniffer policies are used to configure a physical interface on the FortiGate unit as a one-arm intrusion detection system (IDS). Traffic sent to the interface is examined for matches to the configured IPS sensor and application control list. Matches are logged and then all received traffic is dropped. Sniffing only reports on attacks. It does not deny or otherwise influence traffic.

This section describes how to configure your network topology to use the FortiGate unit as a one-arm intrusion detection system. It also describes how to configure and enable a sniffer policy.

The following topics are included in this section:

- [Sniffer policy concepts](#)
- [Before you begin](#)
- [Enable one-arm sniffing](#)
- [Sniffer example](#)

Sniffer policy concepts

Using the one-arm intrusion detection system (IDS), you can configure a FortiGate unit to operate as an IDS appliance by sniffing network traffic for attacks without actually processing the packets.

To configure one-arm IDS, you enable sniffer mode on a FortiGate interface and connect the interface to a hub or to the SPAN port of a switch that is processing network traffic. Then you add DoS policies for that FortiGate interface. Each policy can include a DoS sensor, an IPS sensor, and an application control list to detect attacks and application traffic in the network traffic that the FortiGate interface receives from the hub or switch SPAN port.

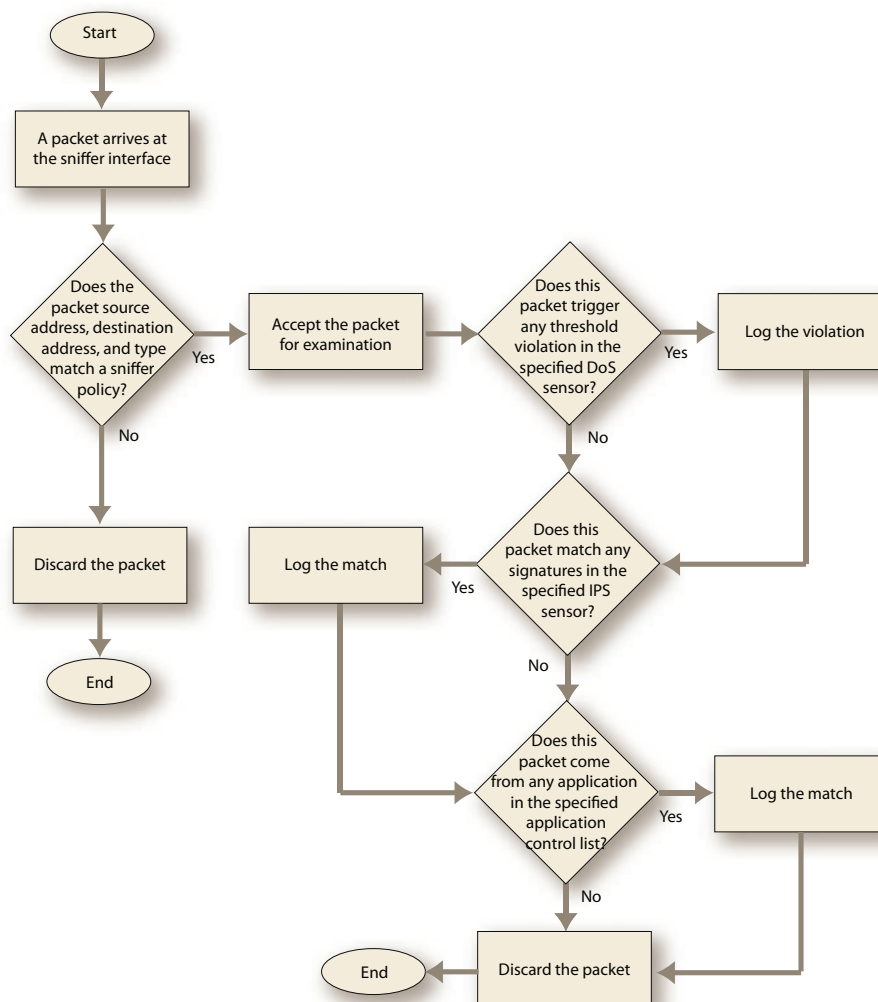
The sniffer policy list

The sniffer policy list shows all of the sniffer policies you have created. The policies are listed by sniffer interface. This is important because multiple sniffer policies can be applied to sniffer interfaces. Traffic entering a sniffer interface is checked against the sniffer policies for matching source and destination addresses and for service. This check against the policies occurs in listed order, from top to bottom. The first sniffer policy matching all three attributes then examines the traffic. Once a policy matches the attributes, checks for policy matches stop. If no sniffer policies match, the traffic is dropped without being examined.

Once a policy match is detected, the matching policy compares the traffic to the contents of the DoS sensor, IPS sensor, and application list specified in the policy. If any matches are detected, the FortiGate unit creates an entry in the log of the matching sensor/list. If the same traffic matches multiple sensors/lists, it is logged for each match. When this comparison is complete, the network traffic is dropped.

[Figure 19](#) illustrates this process.

Figure 19: How the intrusion detection system uses sniffer policies to examine traffic



Before you begin

Traffic entering an interface in sniffer mode is examined for DoS sensor violations, IPS sensor matches, and application control matches. After these checks, all network traffic is dropped. To avoid losing data, you must direct a copy of the network traffic to the FortiGate unit interface configured to sniff packets.

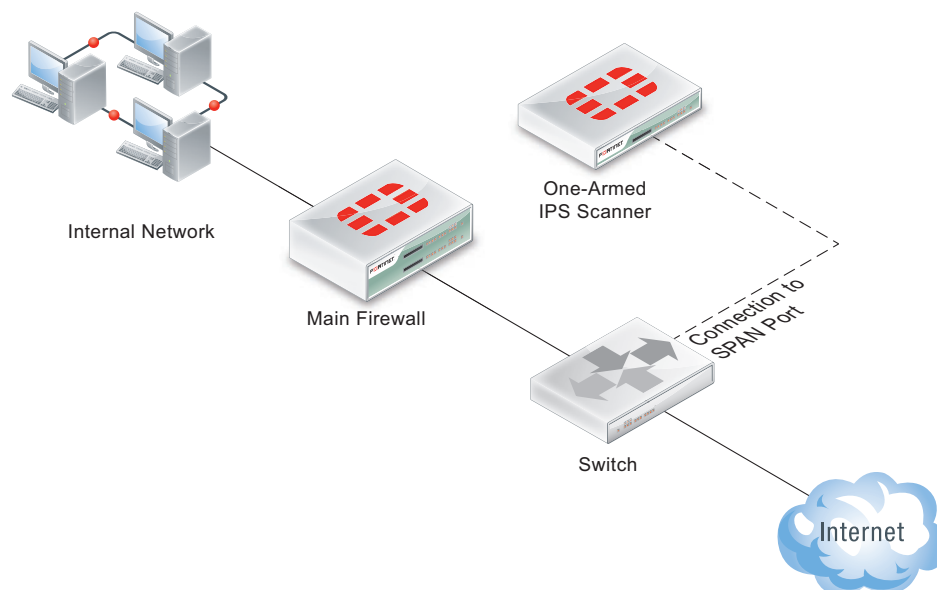
The easiest way to do this is to either use a hub or a switch with a SPAN port.

A hub is the easiest solution to implement but carries a downside. Connecting the FortiGate unit interface configured with the sniffer policy to a hub will deliver all traffic passing through the hub to the interface. However, if the network carries a heavy traffic load, the hub could slow the network because every hub interface sends out all the traffic the hub received on every interface.

A better solution is a switch with a SPAN port. Network switches receive traffic on all interfaces but they only send traffic out on the interface connected to the destination. Network slowdowns are less common when using switches instead of hubs.

Connecting the sniffer interface to a regular switch interface will not work because no traffic is addressed to the sniffer interface. A SPAN port is a special-purpose interface that mirrors all the traffic the switch receives. Traffic is handled normally on every other switch interface, but the SPAN port sends a copy of everything. If you connect your FortiGate unit sniffer interface to the switch SPAN port, all the network traffic will be examined without any being lost because of the examination.

Figure 20: A network configured for intrusion detection using a sniffer policy



Enable one-arm sniffing

Sniffer policies examine network traffic for anomalous patterns that usually indicate an attack. Since all traffic entering a sniffer interface is dropped, you need to first add a switch or hub to your network as described in [“Before you begin” on page 264](#). The following steps are based on the assumption that you have added the switch or hub.

General configuration steps

The interface first must be designated as the sniffer interface, then the sniffer policy can be configured to use the sniffer interface.

- 1 Add a switch or hub to your network as described in [“Before you begin” on page 264](#). This configuration will send a copy of your network traffic to the sniffer interface.



When an interface is configured as a sniffer interface, all traffic received by the interface is dropped after being examined by the sniffer policy.

- 2 Designate a physical interface as a sniffer interface.
- 3 Create a sniffer policy that specifies the sniffer interface.
- 4 Specify a DoS sensor, IPS sensor, application control list, or any combination of the three to define the traffic you want logged.

Designating a sniffer interface

An interface must be designated as a sniffer interface before it can be used with a sniffer policy. Once an interface is designated as a sniffer interface, it functions differently from a regular network interface in two ways:

- A sniffer mode interface accepts all traffic and drops it. If a sniffer policy is configured to use the sniffer interface, traffic matching the attributes configured in the policy will be examined before it is dropped. No traffic entering a sniffer mode interface will exit the FortiGate unit from any interface.
- A sniffer mode interface will be the only available selection in sniffer policies. The sniffer interface will not appear in firewall policies, routing tables, or anywhere else interfaces can be selected.

Designating a sniffer interface

- 1 Go to *System > Network > Interface*.
- 2 Select the interface.
- 3 Select the *Edit* icon.



When an interface is configured as a sniffer interface, all traffic received by the interface is dropped after being examined by the sniffer policy.

- 4 Select the *Enable one-arm sniffer* check box.
If the check box is not available, the interface is in use. Ensure that the interface is not selected in any firewall policies, routes, virtual IPs or other features in which a physical interface is specified.
- 5 Select *OK*.

Creating a sniffer policy

Sniffer interfaces accept all traffic. To examine the traffic before it is dropped, a sniffer policy is required.

To create a sniffer policy

- 1 Go to *Policy > Policy > Sniffer Policy* and select *Create New*.
- 2 For *Source Interface/Zone*, select the interface configured as the sniffer interface. If no interfaces are available for selection, no interfaces have been defined as sniffer interfaces. For more information, see [“Designating a sniffer interface” on page 266](#).
- 3 For *Source Address*, select the address or address group that defines the source addresses of the traffic the sniffer policy will examine. Network traffic from addresses not included in the selected address group is ignored by this sniffer policy.
- 4 For *Destination Address*, select the address or address group that defines the destination addresses of the traffic the sniffer policy will examine. Network traffic to addresses not included in the selected address group is ignored by this sniffer policy.
- 5 For *Service*, select the type of network traffic the sniffer policy will examine. Protocols not included in the selected service or service group are ignored by this sniffer policy.
- 6 To have the sniffer policy log violations specified in a DoS sensor, select the *DoS Sensor* check box and choose the sensor from the list.
- 7 To have the sniffer policy log signatures appearing in an IPS sensor, select the *IPS Sensor* check box and choose the sensor from the list.

- 8 To have the sniffer policy log traffic from applications specified in an application control list, select the *Application Black/White List* check box and choose the application control list.
- 9 Select OK.

DoS sensors, IPS sensors, and application control lists all allow you to choose actions and log traffic. When included in a sniffer sensor, these settings are ignored. Actions in these other settings do not apply, and all matches are logged regardless of the logging setting.

Sniffer example

An IDS sniffer configuration

The Example.com Corporation uses a pair of FortiGate-620B units to secure the head office network. To monitor network attacks and create complete log records of them, the network administrator has received approval to install a FortiGate-82C to record all IPS signature matches in incoming and outgoing network traffic using a sniffer policy. This example details the set-up and execution of this network configuration.

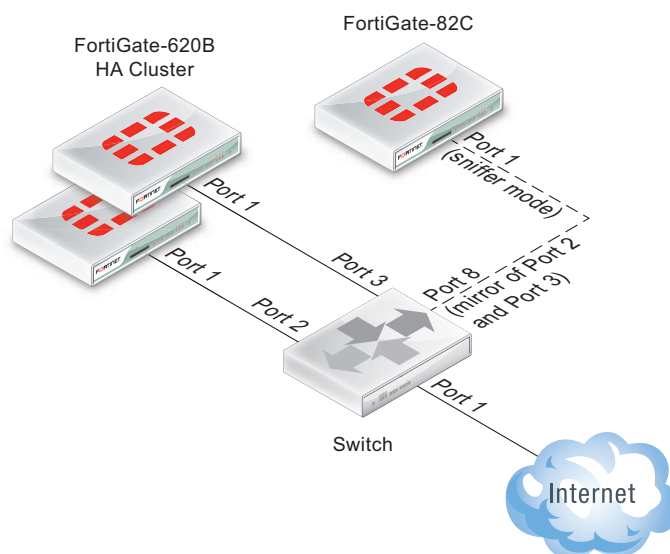
Although this example uses a separate FortiGate unit for sniffer-mode operation, the sniffer traffic can be sent to the FortiGate unit protecting the network. The switch must still be configured to create a copy of the data because the sniffer interface drops all incoming traffic. In this case, the administrator requested a FortiGate-82C for this purpose because sniffer-mode operation is resource intensive, and using a separate FortiGate unit frees the FortiGate-620B cluster from this task. The FortiGate-82C unit also has four internal hard drives, making it ideal for storing large log files.

Configuring the network

Connect the Port1 interface of the FortiGate-82C to the Port8 interface of the switch.

You must configure your network to deliver a copy of the traffic to be examined to the sniffer interface because all network traffic entering a sniffer interface is dropped after examination.

Since the corporate network uses a pair of FortiGate units in an HA cluster, a switch is already in place connecting the Internet to Port1 of both FortiGate units.

Figure 21: Switch configuration

The company Internet feed is connected to Port1 of the switch. The FortiGate units are connected to Port2 and Port3 of the switch. Since they are configured as an HA cluster, they must both have access to the Internet in the event of a failure.

To allow a FortiGate unit sniffer interface to examine the network traffic, the switch must be configured to create a copy of all network traffic entering or leaving Port2 and Port3 and send it out Port8. When configured this way, the switch port sending the duplicate traffic is called a mirror port or a SPAN port.

Consult the switch documentation for instructions on how to configure a SPAN port.



The traffic between Port1 and Port2/Port3 is not modified or diverted in any way by the creation of a SPAN port. The traffic is duplicated with the copy being sent out of the SPAN port.

Configuring the FortiGate sniffer interface

No sniffer interfaces are included in the default configuration of any FortiGate unit. A copy of all of the network traffic is being sent to Port1 of the FortiGate-82C so you must configure Port1 as a sniffer-mode interface.



When an interface is configured as a sniffer interface, all traffic received by the interface is dropped after being examined by the sniffer policy.

To configure the sniffer mode interface — web-based manager

- 1 Log in to the FortiGate-82C web-based manager.
- 2 Go to *System > Network > Interface*.
- 3 Select the Port1 interface.
- 4 Select *Edit*.
- 5 Select *Enable one-arm sniffer*.
- 6 Select *OK*.

To configure the sniffer mode interface — CLI

```
config system interface
  edit port1
    set ips-sniffer-mode enable
  end
```

Creating an IPS sensor

A sniffer policy allows you to select an IPS sensor, a DOS sensor, and an application control list. Any conditions these sensors and list are configured to detect and log are saved to the appropriate log.

For this example, create an IPS sensor that detects and logs the occurrence of all the predefined IPS signatures.

To create an IPS sensor — web-based manager

- 1 Go to *UTM Profiles > Intrusion Protection > IPS Sensor*.
- 2 Select *Create New*.
- 3 In the *Name* field, enter `IPS_sniffer`.
- 4 In the *Comments* field, enter `IPS sensor for use in the sniffer policy`.
- 5 In the *Filters* section, select *Create New*.
- 6 In the name field, enter `All signatures, logged`.
- 7 For the *Logging* setting under *Signatures Settings*, select *Enable all*.
- 8 Select *OK* to save the filter.
- 9 Ensure *Enable Logging* is selected in the sensor.
- 10 Select *OK* to save the IPS sensor.

To create an IPS sensor — CLI

```
config ips sensor
  edit IPS_sniffer
    set comment "IPS sensor for use in the sniffer policy."
  config filter
    edit "All signatures, logged"
      set log enable
    end
  end
```

Creating the sniffer policy

The sniffer policy allows us to choose

To create the sniffer policy — web-based manager

- 1 Go to *Policy > Policy > Sniffer Policy*.
- 2 Select *Create New*.
- 3 Select *Port1* for the *Source Interface/Zone*.
- 4 Enable *IPS Sensor* and select the `IPS_sniffer` sensor.
- 5 Select *OK* to save the sniffer policy.

To create the sniffer policy — web-based manager

```
config firewall sniff-interface-policy
```

```

edit 0
  set interface port1
  set srcaddr all
  set dstaddr all
  set service ANY
  set ips-sensor-status enable
  set ips-sensor IPS_sniffer
end

```

With this configuration, all traffic entering the sniffer port is checked for matching signatures. Matches are logged and the traffic is dropped.

To examine the network traffic for more issues, you can create a DoS sensor and select it in the sniffer policy to log traffic anomalies. You can also create an application list with the specific application you'd like to check for and select it in the sniffer policy.

Sniffer Policy interface reference

The sniffer security policy list displays sniffer security policies in their order of matching precedence for each interface, source/destination address pair, and service.

If virtual domains are enabled on the unit, sniffer security policies are configured separately for each virtual domain; you must access the VDOM before you can configure its security policies.

You can add, delete, edit, and re-order security policies in the sniffer policy list. Sniffer policy order affects policy matching. As with security policies and DoS security policies, sniffer security policies are checked against traffic in the order in which they appear in the sniffer policy list, one at a time, from top to bottom. When a matching policy is discovered, it is used and further checking for sniffer policy matches are stopped. If no match is found the packet is dropped.

Sniffer policy configuration settings

The following are sniffer policy configuration settings in *Policy > Policy > Sniffer Policy*.

Sniffer Policy page	
Lists each individual sniffer policy that you created. On this page, you can edit, delete and create a new sniffer policy. You can also move a policy or insert a new policy on the page.	
Note: All of the specified attributes must match network traffic to trigger the policy.	
Create New	Creates a new sniffer policy. Select the down arrow beside <i>Create New</i> to add a new section to the list to visually group the security policies. When you select <i>Create New</i> (or an option from the down arrow's drop-down list), you are automatically redirected to the New Policy page.
Edit	Modifies settings within the sniffer policy. When you select <i>Edit</i> , you are automatically redirected to the Edit Sniffer Policy page. You can also edit a sniffer policy by selecting the down arrow beside <i>Edit</i> and then selecting <i>Edit Policy</i> . If you want to disable or enable a sniffer policy, select the down arrow beside <i>Edit</i> , and then select either <i>Enable</i> or <i>Disable</i> .

Delete	<p>Removes a policy from the list on the Sniffer Policy page.</p> <p>To remove multiple security policies from within the list, on the Sniffer Policy page, in each of the rows of the security policies you want removed, select the check box and then select <i>Delete</i>.</p> <p>To remove all security policies from the list, on the Sniffer Policy page, select the check box in the check box column, and then select <i>Delete</i>.</p>
Move To	<p>Moves the corresponding policy before or after another policy in the list. When you select <i>Move To</i>, the Move Policy window appears.</p> <p>To move a sniffer policy, select the new position <i>Before</i> or <i>After</i>, which will place the current policy before or after the policy you enter in the field (<i>Policy ID</i>). Enter the policy ID number in the field and then select <i>OK</i>.</p>
Insert	<p>Adds a new policy above the corresponding policy (the New Policy screen appears). See “New Policy page” on page 272.</p>
Filter Settings	<p>Select to filter the information on the page. <i>Filters</i> appears automatically after selecting <i>Filter Settings</i>, below the column headings. Use to configure filter settings.</p> <p>Note: <i>Filter Settings</i> configures all filter settings. Filter icons are used to configure filter settings within that column.</p> <p>To apply a filter setting, select the plus sign beside <i>Add new filter</i> and then select and enter the information required. Repeat to add other filter settings.</p> <p>To modify settings, select <i>Change</i> beside the setting and edit the settings.</p> <p>To clear all filter settings, select the icon beside <i>Clear all filters</i>.</p> <p>To use a filter icon to filter settings within a column, select the filter icon in the column; <i>Filters</i> appears. Within <i>Filters</i>, configure the settings for that column.</p>
Column Settings	<p>Select when you want to Include or remove columns. You can select the columns to hide or display and specify the column displaying order in the table.</p>
Section View	<p>Select to display security policies organized by interface.</p>
Global View	<p>Select to list all security policies in order according to a sequence number.</p>
ID	<p>A unique identifier for each policy. security policies are numbered in the order they are created.</p>
Source	<p>The source address or address group to which the policy applies.</p>
Destination	<p>The destination address or address group to which the policy applies.</p>
Service	<p>The service to which the policy applies.</p>
DoS Sensor	<p>The DoS sensor selected in this policy.</p>

IPS Sensor	The IPS sensor selected in this policy.
Application Control List	The application sensor that is selected in this policy.
Status	When selected, the DoS policy is enabled. Clear the check box to disable the policy.
Interface	The interface used by the policy.
New Policy page Provides settings for configuring a new sniffer policy. When you select <i>Create New</i> on the Sniffer Policy page, you are automatically redirected to this page.	
Source Interface/Zone	The interface or zone to be monitored.
Source Address	Select an address, address range, or address group to limit traffic monitoring to network traffic sent from the specified address or range. Select <i>Multiple</i> to include multiple addresses or ranges. You can also select <i>Create New</i> to add a new address or address group.
Destination Address	Select an address, address range, or address group to limit traffic monitoring to network traffic sent to the specified address or range. Select <i>Multiple</i> to include multiple addresses or ranges. You can also select <i>Create New</i> to add a new address or address group.
Service	Select a firewall pre-defined service or a custom service to limit traffic monitoring to only the selected service or services. You can also select <i>Create New</i> to add a custom service.
DoS sensor	Select and specify a DoS sensor to have the unit apply the sensor to matching network traffic. You can also select <i>Create New</i> within the drop-down list to add a new DoS sensor.
Enable IPS	Select an IPS sensor from the drop-down list. You can also select <i>Create New</i> within the drop-down list to add a new IPS sensor.
Enable Application Control	Select an application sensor from the drop-down list. You can also select <i>Create New</i> within the drop-down list to add a new application sensor.
Enable Antivirus	Select an antivirus profile from the drop-down list. You can also select <i>Create New</i> within the drop-down list to add a new antivirus profile.
Enable Web Filter	Select a web filter profile from the drop-down list. You can also select <i>Create New</i> within the drop-down list to add a new web filter profile.
Enable DLP sensor	Select a DLP sensor from the drop-down list. You can also select <i>Create New</i> within the drop-down list to add a new DLP sensor.



Other UTM considerations

The following topics are included in this section:

- [UTM and Virtual domains \(VDOMs\)](#)
- [Conserve mode](#)
- [SSL content scanning and inspection](#)
- [Viewing and saving logged packets](#)
- [Using wildcards and Perl regular expressions](#)
- [Protocol Options interface reference](#)
- [Offloading UTM processing using Internet Content Adaptation Protocol \(ICAP\)](#)
- [Profile Group interface reference](#)
- [Monitor interface reference](#)

UTM and Virtual domains (VDOMs)

If you enable virtual domains (VDOMs) on your FortiGate unit, all UTM configuration is limited to the VDOM in which you configure it.

While configuration is not shared, the various databases used by UTM features are shared. The FortiGuard antivirus and IPS databases and database updates are shared. The FortiGuard web filter and spam filter features contact the FortiGuard distribution network and access the same information when checking email for spam and web site categories and classification.

Conserve mode

FortiGate units perform all UTM processing in physical RAM. Since each model has a limited amount of memory, conserve mode is activated when the remaining free memory is nearly exhausted or the AV proxy has reached the maximum number of sessions it can service. While conserve mode is active, the AV proxy does not accept new sessions.

The AV proxy

Most content inspection the FortiGate unit performs requires that the files, email messages, URLs, and web pages be buffered and examined as a whole. The AV proxy performs this function, and because it may be buffering many files at the same time, it uses a significant amount of memory. Conserve mode is designed to prevent all the component features of the FortiGate unit from trying to use more memory than it has. Because the AV proxy uses so much memory, conserve mode effectively disables it in most circumstances. As a result, the content inspection features that use the AV proxy are also disabled in conserve mode.

All of the UTM features use the AV proxy with the exception of IPS, application control, DoS as well as flow-based antivirus, DLP, and web filter scanning. These features continue to operate normally when the FortiGate unit enters conserve mode.

Entering and exiting conserve mode

A FortiGate unit will enter conserve mode because it is nearly out of physical memory, or because the AV proxy has reached the maximum number of sessions it can service. The memory threshold that triggers conserve mode varies by model, but it is about 20% free memory. When memory use rises to the point where less than 20% of the physical memory is free, the FortiGate unit enters conserve mode.

The FortiGate unit will leave conserve mode only when the available physical memory exceeds about 30%. When exiting conserve mode, all new sessions configured to be scanned with features requiring the AV proxy will be scanned as normal, with the exception of a unit configured with the one-shot option.

Conserve mode effects

What happens when the FortiGate unit enters conserve mode depends on how you have `av-failopen` configured. There are four options:

off

The off setting forces the FortiGate unit to stop all traffic that is configured for content inspection by UTM features that use the AV proxy. New sessions are not allowed but current sessions continue to be processed normally unless they request more memory. Sessions requesting more memory are terminated.

For example, if a security policy is configured to use antivirus scanning, the traffic it permits is blocked while in conserve mode. A policy with IPS scanning enabled continues as normal. A policy with both IPS and antivirus scanning is blocked because antivirus scanning requires the AV proxy.

Use the off setting when security is more important than a loss of access while the problem is rectified.

pass

The pass setting allows traffic to bypass the AV proxy and continue to its destination. Since the traffic is bypassing the proxy, no UTM scanning that requires the AV proxy is performed. UTM scanning that does not require the AV proxy continues normally.

Use the pass setting when access is more important than security while the problem is rectified.

Pass is the default setting.

one-shot

The one-shot setting is similar to pass in that traffic is allowed when conserve mode is active. The difference is that a system configured for one-shot will force new sessions to bypass the AV proxy even after it leaves conserve mode. The FortiGate unit resumes use of the AV proxy only when the `av-failopen` setting is changed or the unit is restarted.

idledrop

The idledrop setting will recover memory and session space by terminating all the sessions associated with the host that has the most sessions open. The FortiGate may force this session termination a number of times, until enough memory is available to allow it to leave conserve mode.

The idledrop setting is primarily designed for situations in which malware may continue to open sessions until the AV proxy cannot accept more new sessions, triggering conserve mode. If your FortiGate unit is operating near capacity, this setting could cause the termination of valid sessions. Use this option with caution.

Configuring the av-failopen command

You can configure the av-failopen command using the CLI.

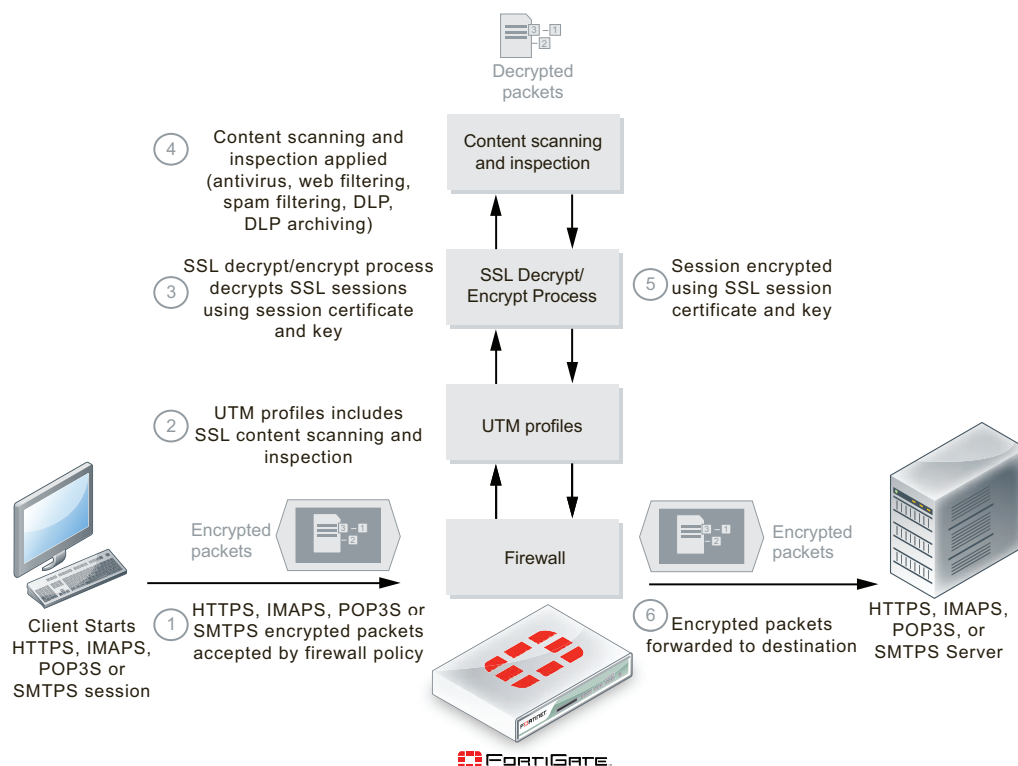
```
config system global
    set av-failopen {off | pass | one-shot | idledrop}
end
```

The default setting is pass.

SSL content scanning and inspection

If your FortiGate model supports SSL content scanning and inspection, you can apply antivirus scanning, web filtering, FortiGuard Web Filtering, and email filtering to encrypted traffic. You can also apply DLP and DLP archiving to HTTPS, IMAPS, POP3S, and SMTPS traffic. To perform SSL content scanning and inspection, the FortiGate unit does the following:

- intercepts and decrypts HTTPS, IMAPS, POP3S, SMTPS, and FTPS sessions between clients and servers (FortiGate SSL acceleration speeds up decryption)
- applies content inspection to decrypted content, including:
 - HTTPS, IMAPS, POP3S, and SMTPS Antivirus, DLP, and DLP archiving
 - HTTPS web filtering and FortiGuard web filtering
 - IMAPS, POP3S, and SMTPS email filtering
- encrypts the sessions and forwards them to their destinations.

Figure 22: FortiGate SSL content scanning and inspection packet flow

Setting up certificates to avoid client warnings

To use SSL content scanning and inspection, you need to set up and use a certificate that supports it. FortiGate SSL content scanning and inspection intercepts the SSL keys that are passed between clients and servers during SSL session handshakes and then substitutes spoofed keys. Two encrypted SSL sessions are set up, one between the client and the FortiGate unit, and a second one between the FortiGate unit and the server. Inside the FortiGate unit the packets are decrypted.

While the SSL sessions are being set up, the client and server communicate in clear text to exchange SSL session keys. The session keys are based on the client and server certificates. The FortiGate SSL decrypt/encrypt process intercepts these keys and uses a built-in signing CA certificate named `Fortinet_CA_SSLProxy` to create keys to send to the client and the server. This signing CA certificate is used only by the SSL decrypt/encrypt process. The SSL decrypt/encrypt process then sets up encrypted SSL sessions with the client and server and uses these keys to decrypt the SSL traffic to apply content scanning and inspection.

Some client programs (for example, web browsers) can detect this key replacement and will display a security warning message. The traffic is still encrypted and secure, but the security warning indicates that a key substitution has occurred.

You can stop these security warnings by importing the signing CA certificate used by the server into the FortiGate unit SSL content scanning and inspection configuration. Then the FortiGate unit creates keys that appear to come from the server and not the FortiGate unit.



You can add one signing CA certificate for SSL content scanning and inspection. The CA certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported for SSL content scanning and encryption.

You can replace the default signing CA certificate, Fortinet_CA_SSLProxy, with another signing CA certificate. To do this, you need the signing CA certificate file, the CA certificate key file, and the CA certificate password.

All SSL content scanning and inspection uses the same signing CA certificate. If your FortiGate unit is operating with virtual domains enabled, the same signing CA certificate is used by all virtual domains.

To add a signing CA certificate for SSL content scanning and inspection

- 1 Obtain a copy of the signing CA certificate file, the CA certificate key file, and the password for the CA certificate.
- 2 Go to *System > Certificates > Local Certificates* and select *Import*.
- 3 Set *Type* to *Certificate*.
- 4 For *Certificate file*, use the *Browse* button to select the signing CA certificate file.
- 5 For *Key file*, use the *Browse* button to select the CA certificate key file.
- 6 Enter the CA certificate *Password*.
- 7 Select *OK*.

The CA certificate is added to the *Local Certificates* list. In this example the signing CA certificate name is *Example_CA*. This name comes from the certificate file and key file name. If you want the certificate to have a different name, change these file names.

- 8 Add the imported signing CA certificate to the SSL content scanning and inspection configuration. Use the following CLI command if the certificate name is *Example_CA*.

```
config firewall ssl setting
  set caname Example_CA
end
```

The *Example_CA* signing CA certificate will now be used by SSL content scanning and inspection for establishing encrypted SSL sessions.

SSL content scanning and inspection settings

If SSL content scanning and inspection is available on your FortiGate unit, you can configure SSL settings. The following table provides an overview of the options available and where to find further instruction:

Table 18: SSL content scanning and inspection settings

Setting	Description
Predefined firewall services	The IMAPS, POP3S and SMTPS predefined services. You can select these services in a security policy and a DoS policy.

Table 18: SSL content scanning and inspection settings (Continued)

Setting	Description
Protocol recognition	<p>The TCP port numbers that the FortiGate unit inspects for HTTPS, IMAPS, POP3S, and SMTPS. Go to <i>Policy > Policy > Protocol Options</i>. Add or edit a protocol options profile, configure HTTPS, IMAPS, POP3S, SMTPS, and FTPS.</p> <p>Using <i>Protocol Options</i>, you can also configure the FortiGate unit to perform URL filtering of HTTPS or to use SSL content scanning and inspection to decrypt HTTPS so that the FortiGate unit can also apply antivirus and DLP content inspection and DLP archiving to HTTPS. Using SSL content scanning and inspection to decrypt HTTPS also allows you to apply more web filtering and FortiGuard Web Filtering options to HTTPS.</p> <p>To enable full SSL content scanning of web filtering, select <i>Enable Deep Scanning</i> under HTTPS in the protocol options profile.</p>
Antivirus	<p>Antivirus options including virus scanning and file filtering for HTTPS, IMAPS, POP3S, and SMTPS.</p> <p>Go to <i>UTM AntiVirus > Profile</i>. Add or edit a profile and configure <i>Virus Scan</i> for HTTPS, IMAPS, POP3S, and SMTPS.</p>
Antivirus quarantine	<p>Antivirus quarantine options to quarantine files in HTTPS, IMAPS, POP3S, SMTPS, and FTPS sessions.</p> <p>Go to <i>UTM Profiles > AntiVirus > Quarantine</i>. You can quarantine infected files, suspicious files, and blocked files found in HTTPS, IMAPS, POP3S, SMTPS, and FTPS sessions.</p>
Web filtering	<p>Web filtering options for HTTPS:</p> <ul style="list-style-type: none"> • Web Content Filter • Web URL Filter • ActiveX Filter • Cookie Filter • Java Applet Filter • Web Resume Download Block • Block invalid URLs <p>Go to <i>UTM Profiles > Web Filter > Profile</i>. Add or edit a web filter profile and configure web filtering for HTTPS.</p>

Table 18: SSL content scanning and inspection settings (Continued)

Setting	Description
FortiGuard Web Filtering	<p>FortiGuard Web Filtering options for HTTPS:</p> <ul style="list-style-type: none"> • Enable FortiGuard Web Filtering • Enable FortiGuard Web Filtering Overrides • Provide Details for Blocked HTTP 4xx and 5xx Errors • Rate Images by URL (Blocked images will be replaced with blanks) • Allow Websites When a Rating Error Occurs • Strict Blocking • Rate URLs by Domain and IP Address • Block HTTP Redirects by Rating <p>Go to <i>UTM Profiles > Web Filter > Profile</i>. Add or edit a profile and configure FortiGuard Web Filtering for HTTPS.</p>
Email filtering	<p>Email filtering options for IMAPS, POP3S, and SMTPS:</p> <ul style="list-style-type: none"> • FortiGuard Email Filtering IP Address Check, URL check, E-mail Checksum Check, and Spam Submission • IP Address BWL Check • E-mail Address BWL Check • Return S-mail DNS Check • Banned Word Check • Spam Action • Tag Location • Tag Format <p>Go to <i>UTM Profiles > Email Filter > Profile</i>. Add or edit a profile and configure email filtering for IMAPS, POP3S, and SMTPS.</p>
Data Leak Prevention	<p>DLP for HTTPS, IMAPS, POP3S, and SMTPS. To apply DLP, follow the steps below:</p> <ul style="list-style-type: none"> • Go to <i>UTM Profiles > Data Leak Prevention > Sensor</i>, create a new DLP sensor or edit an existing one and then add any combination of the DLP advanced rules, DLP compound rules, file filters, a Regular Expressions, and file size limits to a DLP sensor. • Go to <i>Policy > Policy > Protocol Options</i>. Add or edit a profile and select <i>Enable Deep Scan</i> under HTTPS. • Go to <i>Policy > Policy > Policy</i>, edit the required policy, enable UTM, select <i>Enable DLP Sensor</i> and select the DLP sensor. • Go to <i>Policy > Policy > Policy</i>, edit the required policy, enable <i>Protocol Options</i> and select a profile that has <i>Enable Deep Scan</i> selected under HTTPS. Note: If no protocol options profile is selected, or if <i>Enable Deep Scan</i> is not selected within the protocol options profile, DLP rules cannot inspect HTTPS.
DLP archiving	<p>DLP archiving for HTTPS, IMAPS, POP3S, and SMTPS. Add DLP Rules for the protocol to be archived.</p>

Table 18: SSL content scanning and inspection settings (Continued)

Setting	Description
Monitor DLP content information on the system dashboard	<p>DLP archive information on the Log and Archive Statistics widget on the system dashboard for HTTPS, IMAPS, POP3S, and SMTPS.</p> <p>Go to <i>Policy > Policy > Protocol Options</i>. Add or edit a profile. For each protocol you want monitored on the dashboard, enable <i>Monitor Content Information for Dashboard</i>.</p> <p>These options display meta-information on the Statistics dashboard widget.</p>

Viewing and saving logged packets

The FortiGate unit supports packet logging for IPS and application control. The packets that trigger a signature match for IPS or application recognition for application control are saved for later viewing when packet logging is enabled.

For information on how to enable packet logging, see [“Enable IPS packet logging” on page 102](#) and [“Application control packet logging” on page 206](#).

Once the FortiGate unit has logged packets, you can view or save them.

To view and save logged packets

- 1 Go to *Log&Report > Log Access > Attack*.
- 2 Depending on where the logs are configured to be stored, select the appropriate option:

Memory	Select if logs are stored in the FortiGate unit memory.
Disk	Select if the FortiGate unit has an internal hard disk and logs are stored there.
Remote	Select if logs are sent to a FortiAnalyzer unit or to the FortiGuard Analysis and Management Service.

- 3 Select the *Packet Log* icon of the log entry you want to view.
The *IPS Packet Log Viewer* window appears.
 - 4 Select the packet to view the packet in binary and ASCII. Each table row represents a captured packet.
 - 5 Select *Save* to save the packet data in a PCAP formatted file.
- PCAP files can be opened and examined in network analysis software such as Wireshark.

Configuring packet logging options

You can use a number of CLI commands to further configure packet logging.

Limiting memory use

When logging to memory, you can define the maximum amount of memory used to store logged packets.

```
config ips settings
    set packet-log-memory 256
end
```


The acceptable range is from 64 to 8192 kilobytes. This command affects only logging to memory.

Limiting disk use

When logging to the FortiGate unit internal hard disk, you can define the maximum amount of space used to store logged packets.

```
config ips settings
  set ips-packet-quota 256
end
```

The acceptable range is from 0 to 4294967295 megabytes. This command affects only logging to disk.

Configuring how many packets are captured

Since the packet containing the signature is sometimes not sufficient to troubleshoot a problem, you can specify how many packets are captured before and after the packet containing the IPS signature match.

```
config ips settings
  packet-log-history
  packet-log-post-attack
end
```

The `packet-log-history` command specifies how many packets are captured before and including the one in which the IPS signature is detected. If the value is more than 1, the packet containing the signature is saved in the packet log, as well as those preceding it, with the total number of logged packets equalling the `packet-log-history` setting. For example, if `packet-log-history` is set to 7, the FortiGate unit will save the packet containing the IPS signature match and the six before it.

The acceptable range for `packet-log-history` is from 1 to 255. The default is 1.



Setting `packet-log-history` to a value larger than 1 can affect the performance of the FortiGate unit because network traffic must be buffered. The performance penalty depends on the model, the setting, and the traffic load.

The `packet-log-post-attack` command specifies how many packets are logged after the one in which the IPS signature is detected. For example, if `packet-log-post-attack` is set to 10, the FortiGate unit will save the ten packets following the one containing the IPS signature match.

The acceptable range for `packet-log-post-attack` is from 0 to 255. The default is 0.

Using wildcards and Perl regular expressions

Many UTM feature list entries can include wildcards or Perl regular expressions.

For more information about using Perl regular expressions, see <http://perldoc.perl.org/perlretut.html>.

Regular expression vs. wildcard match pattern

A wildcard character is a special character that represents one or more other characters. The most commonly used wildcard characters are the asterisk (*), which typically represents zero or more characters in a string of characters, and the question mark (?), which typically represents any one character.

In Perl regular expressions, the '.' character refers to any single character. It is similar to the '?' character in wildcard match pattern. As a result:

- example.com not only matches example.com but also examplea.com, exampleb.com, examplec.com, and so on.



To add a question mark (?) character to a regular expression from the FortiGate CLI, enter Ctrl+V followed by ?. To add a single backslash character (\) to a regular expression from the CLI you must add precede it with another backslash character. For example, `example\\.com`.

To match a special character such as '.' and '*' use the escape character '\\'. For example:

- To match example.com, the regular expression should be: `example\\.com`

In Perl regular expressions, '*' means match 0 or more times of the character before it, not 0 or more times of any character. For example:

- `exam*.com` matches `exammmmm.com` but does not match `example.com`

To match any character 0 or more times, use '.' where '.' means any character and the '*' means 0 or more times. For example, the wildcard match pattern `exam*.com` should therefore be `exam.*\\.com`.

Word boundary

In Perl regular expressions, the pattern does not have an implicit word boundary. For example, the regular expression "test" not only matches the word "test" but also any word that contains "test" such as "atest", "mytest", "testimony", "atestb". The notation "\\b" specifies the word boundary. To match exactly the word "test", the expression should be `\\btest\\b`.

Case sensitivity

Regular expression pattern matching is case sensitive in the web and Email Filter filters. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` will block all instances of "bad language", regardless of case.

Perl regular expression formats

Table 19 lists and describes some example Perl regular expressions.

Table 19: Perl regular expression formats

Expression	Matches
<code>abc</code>	"abc" (the exact character sequence, but anywhere in the string)
<code>^abc</code>	"abc" at the beginning of the string
<code>abc\$</code>	"abc" at the end of the string
<code>a b</code>	Either "a" or "b"
<code>^abc abc\$</code>	The string "abc" at the beginning or at the end of the string
<code>ab{2,4}c</code>	"a" followed by two, three or four "b"s followed by a "c"
<code>ab{2,}c</code>	"a" followed by at least two "b"s followed by a "c"
<code>ab*c</code>	"a" followed by any number (zero or more) of "b"s followed by a "c"
<code>ab+c</code>	"a" followed by one or more b's followed by a c

Table 19: Perl regular expression formats (Continued)

ab?c	“a” followed by an optional “b” followed by a “c”; that is, either “abc” or “ac”
a.c	“a” followed by any single character (not newline) followed by a “c”
a\.c	“a.c” exactly
[abc]	Any one of “a”, “b” and “c”
[Aa]bc	Either of “Abc” and “abc”
[abc]+	Any (nonempty) string of “a”s, “b”s and “c”s (such as “a”, “abba”, “acbabcacaa”)
[^abc]+	Any (nonempty) string which does not contain any of “a”, “b”, and “c” (such as “defg”)
\d\d	Any two decimal digits, such as 42; same as \d{2}
/i	Makes the pattern case insensitive. For example, /bad language/i blocks any instance of bad language regardless of case.
\w+	A “word”: A nonempty sequence of alphanumeric characters and low lines (underscores), such as foo and 12bar8 and foo_1
100\s*mk	The strings “100” and “mk” optionally separated by any amount of white space (spaces, tabs, newlines)
abc\b	“abc” when followed by a word boundary (for example, in “abc!” but not in “abcd”)
perl\b	“perl” when not followed by a word boundary (for example, in “perlert” but not in “perl stuff”)
\x	Tells the regular expression parser to ignore white space that is neither preceded by a backslash character nor within a character class. Use this to break up a regular expression into (slightly) more readable parts.
/x	Used to add regular expressions within other text. If the first character in a pattern is forward slash '/', the '/' is treated as the delimiter. The pattern must contain a second '/'. The pattern between '/' will be taken as a regular expressions, and anything after the second '/' will be parsed as a list of regular expression options ('i', 'x', etc). An error occurs if the second '/' is missing. In regular expressions, the leading and trailing space is treated as part of the regular expression.

Examples of regular expressions

Block any word in a phrase

```
/block|any|word/
```

Block purposely misspelled words

Spammers often insert other characters between the letters of a word to fool spam blocking software.

```
/^.*v.*i.*a.*g.*r.*o.*$/i
```

```
/cr[eéeêë] [\+ \- \* = < > \. \, ; ! \? % & $ @ \^ ° \ $ £ € \{ \} () \[ \] \ | \ \ 01]dit/i
```

Block common spam phrases

The following phrases are some examples of common phrases found in spam messages.

```
/try it for free/i
```

```
/student loans/i
```

```
/you're already approved/i
```

```
/special[\+\-\*=<>\.\,;!\?%&~#\$@\^\°\$£€\{\}\(\)\[\]\|\\_1]offer/i
```

Protocol Options interface reference

The Protocol Options menu allows you to configure settings for specific protocols, which are grouped together in a protocol group, and then applied to a security policy. The default groups are scan, strict, unfiltered, and web.

Protocol options configuration settings

The following are protocol option configuration settings in *Policy > Policy > Protocol Options*.

Protocol Options page Lists each individual protocol setting that you created. On this page, you can edit, delete or create a new group of protocol settings. Note: If you want to provide information about any of the protocols, select the check box beside <i>Monitor Content Information for Dashboard</i> , which is available within each protocol section.	
Create New	Creates a new protocol option. When you select <i>Create New</i> , you are automatically redirected to the Protocol Options Settings page.
Edit	Modifies settings to a protocol setting. When you select <i>Edit</i> , you are automatically redirected to the Protocol Options page.
Delete	Removes a protocol setting from the list on the Protocol Options page. To remove multiple protocol settings from within the list, on the Protocol Options page, in each of the rows of the policies you want removed, select the check box and then select <i>Delete</i> . To remove all protocol options from the list, on the Protocol Options page, select the check box in the check box column, and then select <i>Delete</i> .
Name	The name of the protocol group. This group is the group you select when applying it to a security policy.
Comments	Describes the protocol group.

Ref.	<p>Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a security policy; on the Profile page (<i>UTM Profiles > Antivirus > Profile</i>), 1 appears in <i>Ref.</i>.</p> <p>To view the location of the referenced object, select the number in <i>Ref.</i>, and the Object Usage window appears displaying the various locations of the referenced object.</p> <p>To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:</p> <ul style="list-style-type: none"> • View the list page for these objects – automatically redirects you to the list page where the object is referenced at. • Edit this object – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy and so, when the icon is selected, the user is redirected to the Edit Policy page. • View the details for this object – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy, and that security policy's settings appear within the table.
<p>Protocol Options Settings page</p> <p>Provides settings for configuring options for each protocol which make up a protocol group.</p> <p>Note: There are similar settings within each protocol setting.</p>	
Name	Enter a name for the protocol group.
Comments	Enter a description about the protocol group. This is optional.
Enable Oversized File Log	Select to allow logging of oversized files.
Enable Invalid Certificate Log	Select to allow logging of invalid certificates.
HTTP section	Configure settings for the HTTP protocol or the HTTPS protocol.
Port (i.e. 80,88, 0-auto)	This is available for every protocol except for IM.
Comfort Clients	<p>This is available only for HTTP, FTP, and HTTPS.</p> <ul style="list-style-type: none"> • Interval (1-900 seconds) – enter the interval time in seconds. • Amount (1-10240 bytes) – enter the amount in bytes.
Oversized File/Email	<p>This is available for all protocols.</p> <ul style="list-style-type: none"> • Threshold – enter the threshold amount for an oversized email message or file in MB.

Monitor Content Information for Dashboard	Select to view the activity of the protocol from the Dashboard menu.
Enable Chunked Bypass	Select to enable the chunked bypass setting.
FTP section	Configure settings for the file transfer protocol. <i>FTP</i> and <i>HTTP</i> contain the same settings, except the FTP section does not contain the option <i>Enable Chunked Bypass</i> .
FTPS section	Configure settings for the FTPS protocol. FTPS is an extension of the FTP protocol, adding support for both the TLS and SSL cryptographic protocols. This section contains the same settings as in the <i>FTP</i> section.
IMAP section	Configure settings for the IMAP protocol.
Allow Fragmented Messages	Allows fragmented email messages to be passed.
POP3 section	Configure settings for the POP3 protocol. This section contains the same settings as are in the IMAP section.
SMTP section	Configure settings for the SMTP section.
Append Email Signature	Select to enable the option of entering a new email signature that appears in the email message.
Email Signature Text	Enter a signature for the email message, for example, Yours sincerely. Accessible only when Append Email Signature is selected.
IM section	Configure settings for the IM protocol.
NNTP section	Configure settings for the NNTP protocol.
HTTPS section	Configure settings for the HTTPS protocol.
Allow Invalid SSL Certificate	Select to allow invalid SSL certificates.
Enable Deep Scanning	Select to allow deep scanning.
IMAPS	Configure settings for the IMAPS protocol.
POP3S	Configure settings for the POP3S protocol. This section contains the same settings as <i>IMAPS</i> .
SMTPS	Configure settings for the SMTPS protocol. This section contains the same settings as <i>IMAPS</i> and <i>POP3S</i> .

Offloading UTM processing using Internet Content Adaptation Protocol (ICAP)

The Internet Content Adaptation Protocol (ICAP) is supported in this release. ICAP is a light-weight response/request protocol that allows the FortiGate unit to offload HTTP and HTTPS traffic to external servers for different kinds of processing. ICAP is often used for offloading UTM features such as virus scanning, DLP and web filtering but has many other applications.



ICAP does not appear by default in the web-based manager. You must enable it in *System > Admin > Settings* to display ICAP in the web-based manager.

If you enable ICAP in a security policy, HTTP traffic intercepted by the policy is transferred to an ICAP server in the ICAP profile added to the policy. Responses from the ICAP server are returned to the FortiGate unit which forwards them to an HTTP client or server.

You can offload HTTP responses or HTTP requests (or both) to the same or different ICAP servers.

If the FortiGate unit supports HTTPS inspection, HTTPS traffic intercepted by a policy that includes an ICAP profile is also offloaded to the ICAP server in the same way as HTTP traffic.

Example ICAP sequence for an ICAP server performing web URL filtering on HTTP requests

- 1 A user opens a web browser and sends an HTTP request to connect to a web server.
- 2 The FortiGate unit intercepts the HTTP request and forwards it to an ICAP server.
- 3 The ICAP server receives the request and determines if the request is for URL that should be blocked or allowed.
 - If the URL should be blocked the ICAP server sends a response to the FortiGate unit. The FortiGate unit returns this response to the user's web browser. This response could be a message informing the user that their request was blocked.
 - If the URL should be allowed the ICAP server sends a request to the FortiGate unit. The FortiGate unit forwards the request to the web server that the user originally attempted to connect to.

When configuring ICAP on the FortiGate unit, you must configure an ICAP profile that contains the ICAP server information; this profile is then applied to a security policy.

Example of adding ICAP to a security policy

The following is an example of configuring the ICAP feature on the FortiGate unit and applying an ICAP profile to an existing security policy.

- 1 Log in to the CLI.
- 2 Enter the following to configure the ICAP server:

```
config icap server
edit icap_server
set ip-address 172.16.122.151
set ip-version 4
set max-connections 25
set port 453
```

```
end
```

- 3** Enter the following to configure the ICAP profile to then apply to a security policy:

```
config icap profile
  edit icap_profile_1
    set request enable
    set request-failure error
    set request-path 1220
    set request-server icap_server
    set response enable
    set response-failure error
    set response-path 1225
    set response-server 172.16.122.151
    set streaming-content-bypass enable
  end
```

- 4** In the `config firewall policy` command, apply the ICAP profile to policy 1:

```
config firewall policy
  edit 1
    set icap-profile icap_profile_1
  end
```

Troubleshooting ICAP

You can use the following diagnose commands when troubleshooting ICAP.

```
diag system icap server list <name>
```

Displays a list of all servers or specified servers.

```
diag system icap profile list <name>
```

Displays information concerning total sent and responses, last connection attempts and host-bypass count.

ICAP profile

The following are ICAP profile configuration settings in *UTM Profiles > ICAP > Profile*.

ICAP Profile page Lists each ICAP profile that you created. On this page, you can edit, delete and create a new ICAP profiles. Note: Logging is enabled in the CLI.	
Name	Enter the name of the new ICAP profile.
Enable Request Processing	Select to enable how the request from an ICAP server will be processed by the unit.
Server	Select the ICAP server from the drop-down list. An ICAP server must be configured before you can configure an ICAP profile. See “ICAP server” on page 289 .
Path	Enter the path name.
On Failure	Select either <i>Error</i> or <i>Bypass</i> . This instructs the unit on which action to take if a failure occurs.
Enable Response Processing	Select to enable how the response from an ICAP server will be processed by the unit.

Server	Select the ICAP server from the drop-down list. An ICAP server must be configured before you can configure an ICAP profile. See “ICAP server” on page 289 .
Path	Enter the path name.
On Failure	Select either <i>Error</i> or <i>Bypass</i> . This instructs the unit on which action to take if a failure occurs.
Enable Streaming Media Bypass	Select to enable streaming media bypass.

ICAP server

The following are ICAP server configuration settings in *UTM Profiles > ICAP > Server*.

ICAP Server page	
Lists each ICAP profile that you created. On this page, you can edit, delete and create a new ICAP profiles.	
Note: Logging is enabled in the CLI.	
Name	Enter the name of the new ICAP profile.
IP Type	Enter the type of IP address the ICAP server uses, either IPv4 or IPv6.
IP Address	Enter the IP address of the ICAP server.
Port	Enter the port that the ICAP server uses.

Profile Group interface reference

A profile group is a group of UTM features that include MMS profiles and replacement message groups. You can configure multiple profile groups, which are then applied to a firewall policy. This provides an easier way to apply multiple profiles and sensors to a firewall policy.

Profile Group configuration settings

The following are profile group configuration settings. If you are running FortiOS Carrier, these configuration settings are in *UTM Profiles > Carrier > Profile Group*; however, if you are running FortiOS, these configuration settings are in *UTM Profiles > Profile Group > Profile Group*.

Profile Group page	
Lists all the profile groups that you have created. On this page, you can edit, delete or create a new profile group.	
Create New	Creates a new profile group. When you select <i>Create New</i> , you are automatically redirected to the New Profile Group page.
Edit	Modifies a profile group's settings. When you select <i>Edit</i> , you are automatically redirected to the Edit Profile Group page.

Delete	<p>Removes a profile group from the list.</p> <p>To remove multiple profile groups from within the list, on the Profile Group page, in each of the rows of the groups you want removed, select the check box and then select <i>Delete</i>.</p> <p>To remove all profile groups from the list, on the Profile Group page, select the check box in the check box column and then select <i>Delete</i>.</p>
Name	The name of the profile group.
New Profile Group page Provides settings for configuring a profile group. You must configure UTM features prior to configuring a profile group because profile groups require these UTM features. If you want to include a replacement message group, that group must also be configured prior to configuring a profile group. You cannot configure a UTM feature or replacement group from the New Profile Group page.	
Name	Enter a name for the profile group.
Protocol Options	Select the check box to enable this option and then select a protocol option from the drop-down list. Protocol options are configured in <i>Firewall > Policy > Protocol Options</i> .
Enable Antivirus	Select the check box to enable this option and then select an antivirus profile from the drop-down list. Antivirus profiles are configured in <i>UTM Profiles > Antivirus > Profile</i> .
Enable IPS	Select the check box to enable this option and then select the IPS sensor from the drop-down list. IPS sensors are configured in <i>UTM Profiles > Intrusion Protection > IPS Sensor</i> .
Enable Web Filter	Select the check box to enable this option and then select the web filter profile from the drop-down list. Web filter profiles are configured in <i>UTM Profiles > Web Filter > Profile</i> .
Enable Email Filter	Select the check box to enable this option and then select the email filter profile from the drop-down list. Email filter profiles are configured in <i>UTM Profiles > Email Filter > Profile</i> .
Enable DLP Sensor	Select the check box to enable this option and then select the DLP sensor from the drop-down list. DLP sensors are configured in <i>UTM Profiles > Data Leak Prevention > Sensors</i> .
Enable Application Control	Select the check box to enable this option and then select the application control list from the drop-down list. Application control lists are configured in <i>UTM Profiles > Application Control > Application Control Lists</i> .
Enable VoIP	Select the check box to enable this option and then select the VoIP profile from the drop-down list. VoIP profiles are configured in <i>UTM Profiles > VoIP > Profile</i> .
Enable MMS Profile	Select the check box to enable this option and then select the MMS profile from the drop-down list. MMS profiles are configured in <i>UTM Profiles > Carrier > MMS Profile</i> .
Enable Replacement Message Group	Select the check box to enable this option and then select the replacement message group from the drop-down list. Replacement message groups are configured in <i>System > Config > Replacement Message Group</i> .

Monitor interface reference

The Monitor submenus allow you to view the UTM activity occurring on your network. You must have UTM profiles and sensors applied to firewall policies, as well as logging enabled for the profiles and sensors, for the monitors to display any information regarding this activity.

This topic contains the following:

- [AV Monitor](#)
- [Intrusion Monitor](#)
- [Web Monitor](#)
- [Email Monitor](#)
- [Archive & Data Leak Monitor](#)
- [Application Monitor](#)

AV Monitor

The AV Monitor submenu allows you to view statistical information regarding viruses that were detected on your unit from *UTM Profiles > Monitor > AV Monitor*. The information displays in a bar chart as well as in a table below the bar chart. The table contains detailed information.



You must have antivirus logging enabled for this within the profile itself, as well as within log settings and an antivirus profile is applied to a firewall policy.

AV Monitor page

Displays monitored information about viruses that were detected by the unit.

Tip: To view information about a specific virus, select a bar within the chart; the virus FortiGuard definition displays.

Refresh	Select to refresh the information on the page.
Reset	Select to reset the information to clear the current information from the page. New information is included on the page.
Top Viruses (all policies) since <yyyy-mm-dd hh:mm:ss>	The top viruses detected by the unit using all firewall policies.
#	The order that the viruses are listed in the table.
Virus Name	The name of the virus.
Last Detected	The last time that the virus was detected.
Count	The number of times the virus has been detected.

Intrusion Monitor

The Intrusion Monitor submenu allows you to view statistical information regarding attacks that were detected on your unit from *UTM Profiles > Monitor > Intrusion Monitor*. The information displays in a bar chart as well as in a table below the bar chart. The table contains detailed information.

Intrusion Monitor page	
Displays monitored information about attacks that were detected by the unit.	
Tip: To view information about a specific attack, select a bar within the chart; the attack FortiGuard definition displays.	
Refresh	Select to refresh the information on the page.
Reset	Select to reset the information to clear the current information from the page. New information is included on the page.
Top Attacks (all policies) since <yyyy-mm-dd hh:mm:ss>	A bar chart displaying the top attacks detected by the unit.
#	The order that the attacks are listed in the table.
Attack Name	The name of the attack.
Last Detected	The last time that the attack was detected.
Count	The number of times the attack has been detected.

Web Monitor

The Web Monitor submenu allows you to view statistical information regarding the web activity from *UTM Profiles > Monitor > Web Monitor*. The information displays in both a pie chart and a bar chart

Web Monitor page	
Displays monitored information about web activity detected by the unit.	
Refresh	Select to refresh the information on the page.
Reset	Select to reset the information to clear the current information from the page. New information is included on the page.
Report By	Select whether to view the web filter monitored information by web filter technique or by FortiGuard web filter category. If you choose FortiGuard web filter category, you are viewing the information that was gathered from the category settings for FortiGuard web filter from the web filter profile.
Web Monitor since <yyyy-mm-dd hh:mm:ss>	
Total Requests (HTTP)	A pie chart representing the total requests detected.

Blocked Requests (HTTP)	A bar chart representing the total blocked requests detected. The information is broken down to spam, banned words, file filter, viruses, archives, FortiGuard, URL filter, and fragmented.
Total Web Requests (HTTP): <number>	The total number of web requests over HTTP that occurred.

Email Monitor

The Email Monitor submenu allows you to view statistical information regarding email filtering from *UTM Profiles > Monitor > Email Monitor*. The information displays in both a pie chart and bar chart.

Email Monitor page Displays monitored information about email filter activity detected by the unit.	
Refresh	Select to refresh the information on the page.
Reset	Select to reset the information to clear the current information from the page. New information is included on the page.
Total Emails	A pie chart representing the total number of emails scanned by the unit.
Blocked Emails	A bar chart representing the total number of blocked emails, broken down by protocol. The colors indicate the type of scanning that occurred.
Total Emails: <number>	The total number of email messages detected by the unit.

Archive & Data Leak Monitor

The Archive & Data Leak Monitor submenu allows you to view statistical information regarding log archives, as well as DLP usage. This page displays the information in a bar chart in *UTM Profiles > Monitor > Archive & Data Leak Monitor*.

Archive & Data Leak Monitor page Displays monitored information about archive and DLP activity detected by the unit.	
Refresh	Select to refresh the information on the page.
Reset	Select to reset the information to clear the current information from the page. New information is included on the page.
Report By:	Select what type of DLP information you want to view. You can view DLP usage by DLP sensor, firewall policy usage, or by protocol.
Top DLP Usage by DLP Sensor <yyyy-mm-dd hh:mm:ss>	The bar chart that displays DLP usage monitored using DLP sensor information.

Top DLP Usage by Policy <yyyy-mm-dd hh:mm:ss>	The bar chart that displays DLP usage monitored using firewall policy traffic information.
Top DLP Usage by Protocol <yyyy-mm-dd hh:mm:ss>	The bar chart that displays DLP usage monitored using protocol information.
Total Dropped Archives: <number>	The total number of dropped DLP archives.

Application Monitor

The Application Monitor submenu allows you to view statistical information regarding application usage in *UTM Profiles > Monitor > Application Monitor*.

Application Monitor page Displays monitored information about the application usage detected by the unit. Tip: To view top source IP addresses for a specific application, select a bar in the chart to view that application's source IP addresses.	
Refresh	Select to refresh the information on the page.
Reset	Select to reset the information to clear the current information from the page. New information is included on the page.
Top Application Usage by <yyyy-mm-dd hh:mm:ss>	The bar chart that displays the top applications being used detected by the unit.
Resolve Host Name	Appears after selecting a bar for a specific application, for example SSL. Select to resolve the host name. Tip: Hover your mouse over the bar to view the address and total MB (or KB) used for that application.
Report By:	Appears after selecting a bar for a specific application, for example, SSL. Select to view the detailed information by destination address, or source address.
Display User Name	Appears after selecting <i>Source Address</i> from the drop-down list beside <i>Report By</i> . Select to display user names.

FortiGuard Quota

The FortiGuard Quota submenu allows you to view statistical information regarding quota usage by users in *UTM Profiles > Monitor > FortiGuard Quota*.

FortiGuard Quota page Lists the users and the amount of quota that they have used.	
Page Controls	Use to navigate through the list.

User Name	The user name of the user that has FortiGuard quota enabled for them.
Webfilter Profile	The web filter profile that was used for detecting users' FortiGuard quota usage.
Used Quota	The amount of used quota by a user.

Endpoint Monitor

You can view monitored endpoints in *UTM Profiles > Monitor > Endpoint Monitor*. An endpoint is added to the list when it uses a security policy that has *Endpoint Security* enabled.

Endpoint Monitor page Provides information about endpoints, such as endpoint traffic. Note: The pie chart displays information in percent and indicates which is non-compliant and which is compliant.	
Refresh	Updates the list, providing current endpoints that are being monitored.
Report By	Select to view endpoint information by traffic, status or application usage. When you select <i>Status</i> , a pie chart appears along with information about the total endpoints (<i>Total Endpoints</i>). When you select <i>Traffic</i> or <i>Application usage</i> , a bar chart appears; select a bar to view detailed information.

Index

A

- adding, configuring defining
 - anomalies, 124
 - antivirus profile, 46
 - browser cookie-based FortiGuard web filtering overrides, 153
 - custom signature, 130
 - custom signatures, 130
 - DLP document fingerprinting, 190
 - DLP file filter, 192, 193
 - DLP sensor, 186
 - document sources, 191
 - DoS firewall policy, 222
 - DoS sensor, 123
 - email address black/white list, 76
 - email filter banned word, 70
 - email filter black/white IP address list, 73
 - email filter profile, 66
 - endpoint profile, 241
 - endpoint vulnerability result, 262
 - endpoint, asset definition, 260
 - endpoint, client installers, 246
 - endpoint, scan schedule, 261
 - IPS filters, 119
 - IPS sensor, 116
 - pre-defined overrides and custom overrides, 120
 - profile group, 289
 - protocol options, 284
 - sniffer firewall policy, 270
 - tags, application control, 213
 - URL filter, 153
 - web filter local ratings, 157
 - web filter profile, 147
- allow
 - pattern, 178
- anomalies
 - IPS, 125
- anomaly protection
 - DoS, 16
- antispam, **see** email filtering **and** FortiGuard, AntiSpam
- antispam. **See also** Email filter, 64
- antivirus, 31
 - archive scan depth, 38
 - change default database, 36
 - concepts, 31
 - databases, 34
 - enabling scanning, 36
 - example, 43
 - file filtering, 15
 - flow-based scanning, 32
 - FortiAnalyzer, 15
 - HTTPS, IMAPS, POP3S, SMTPS, 278
 - maximum file size, 39
 - override default database, 37
 - proxy-based scanning, 31
 - scan buffer size, 38
 - scanning order, 32
 - virus database, 47
 - virus list, 115
- antivirus monitor, 291
- antivirus profile, 46
- antivirus quarantine
 - HTTPS, IMAPS, POP3S, SMTPS, 278
- application
 - database, viewing, 233
 - detection, 229
- application control, 16, 209
 - monitor, 205
 - packet logging, 206
- application database
 - endpoint, 243
- application monitor, 205, 294
- archive and data leak monitor, 293
- archive antivirus scan depth, 38
- archiving
 - DLP, 182
- assets
 - adding manually, 250
 - discovering, 249
 - selecting to scan, 249

B

- banned user list
 - quarantining attackers, 121
- banned word (spam filter)
 - list, 72
- black list, 16
- block
 - pattern, 178
- blocking of users
 - Endpoint Control, 226
- browser cookie-based overrides
 - FortiGuard web filtering, 152

buffer size
IPS, 102

C

CA certificate, 276
certificate
key size, 277
SSL, 276
concepts
antivirus, 31
web filtering, 16
configuring anomalies, 124
conserve mode, 273
content archiving
DLP archiving, 196
content scanning
SSL, 275
custom signature
adding, 85

D

data leak prevention (DLP), 186
data leak prevention (DLP), **see** DLP
data leak protection, 185
deep scan, 278
deep scanning
firewall protocol, HTTPS, 286
diag system icap profile list , ICAP, 288
diag system icap server list , ICAP, 288
DLP, 171
archiving, 182, 196
content archiving, 196
creating rules, 181, 182
default rules, 180
document fingerprinting, 190
document sources, document fingerprinting, 191
file filter, 192
sensor, 186
DLP archive
displaying on dashboard, 280
HTTPS, IMAPS, POP3S, SMTPS, 279
DLP archiving, 196
DLP. *See* data leak protection
document fingerprinting, 190
DoS
anomaly protection, 16
DoS policy
viewing, 221
DoS sensor
configuring, 123

E

EICAR, 42
email address black/white list, 76
email filter, 64, 76
banned word, 70
order of, 65
IMAP/POP3/IMAPS/POP3S, 66
SMTP/SMTPS, 65
profile, 66

email filtering
IMAPS, POP3S, SMTPS, 279
email filtering, **see also** FortiGuard, AntiSpam, 16
email monitor, 293
endpoint
application database, 243
asset definition, 260
client installers, 246
configuring a profile, 241
scan schedule, 261
vulnerability result, 262
Endpoint Control
blocked users, 226
modifying download portal, 236
modifying recommendation portal, 236
modifying replacement pages, 236
monitoring endpoints, 235
endpoints
monitoring, 235
engine algorithm
IPS, 101
engine count
IPS, 101
example
Endpoint Control configuration, 237

F

fail-open
IPS, 101
file block
default list of patterns, 192
file filtering, 178
antivirus, 15
general configuration steps, 178
file pattern, 32, 178
creating, 179
file quarantine
configuring, 41
general configuration steps, 41
file size, 32
file type, 32, 178
creating, 179
filter
IPS, 81
filtering
using filter settings, 271
fingerprint
DLP, 176
document fingerprint, 176
firewall
DoS policy, 222
protocol options, configuring, 284
sniffer policy, 270
firewall policies
and Endpoint Control, 234
firewall policy, 38
FortiAnalyzer
antivirus, 15
quarantine, 41

- FortiClient
 - download location, 227
 - endpoint, 246
 - required version, 227
- FortiGate-ASM-S08 module, 41
- FortiGate-ASM-SAS module, 41
- FortiGuard
 - AntiSpam, 16
 - Antivirus, 35, 41
 - as source of antivirus signatures, 227
 - as source of application signatures, 227
 - as source of FortiClient installer, 227
 - Web Filtering, 16, 279
 - HTTPS, 279
- FortiGuard Center, 35
- FortiGuard quota, monitoring, 294
- FortiGuard Web Filter quota, 163
- FortiGuard web filtering overrides
 - browser cookie based, 152
- FortiGuard, Distribution Network, 35

G

- general configuration steps
 - file filtering, 178
 - file quarantine, 41
- grayware, 32, 35
 - scanning, 42

H

- HA
 - IPS processing, 100
- heuristics, 32, 35
- HTTPS
 - antivirus, 278
 - antivirus quarantine, 278
 - data leak prevention, 279
 - DLP archive, 279
 - FortiGuard Web Filtering, 279
 - protocol recognition, 278
 - web filtering, 278

I

- ICAP, 287
 - example of ICAP, 287
 - troubleshooting, 288
- IDS
 - one-armed IDS, 16
- IM, 16
- IMAPS
 - antivirus, 278
 - antivirus quarantine, 278
 - data leak prevention, 279
 - DLP archive, 279
 - email filtering, 279
 - predefined firewall services, 277
 - protocol recognition, 278

- inspection
 - SSL, 275
- intrusion detection system, **see** IDS
- intrusion monitor, 292
- intrusion prevention system, **see** IPS
- intrusion protection
 - signatures, 126
- intrusion protection system, **see** IPS
- IP address
 - email filter black/white IP address list, 73
- IPS
 - adding custom signatures, 85
 - buffer size, 102
 - concepts, 79
 - creating tags, 120
 - creating tags for predefined signatures, 128
 - custom signature, 130
 - custom signature keywords, 87
 - custom signature syntax, 86
 - engine algorithm, 101
 - engine count, 101
 - fail-open, 101
 - filter, 81
 - filters, 119
 - in an HA cluster, 100
 - overview, 15
 - packet logging, 102
 - pre-defined overrides and custom overrides, 120
 - protocol decoder, 131
 - scanning, 81
 - sensor, 81, 116
 - session count accuracy, 101
 - SYN
 - threshold, 125
 - SYN proxy, 125
 - understanding anomalies, 125
 - upgrading protocol decoder list, 131
 - viewing predefined signatures, 127
- IPS signature
 - override, 84

K

- key size
 - certificate, 277
- keywords
 - IPS custom signatures, 87

L

- logging
 - IPS packets, 119

M

- maximum file size
 - antivirus, 39
- monitor
 - application control, 205

- monitoring
 - antivirus, 291
 - applications, 294
 - archives and dlp, 293
 - attacks, 292
 - email activity, 293
 - endpoints, 295
 - FortiGuard quota, 294
 - ips, 292
 - web activity, 292

N

- network vulnerability scan
 - asset definition, 260
 - scan schedule, 261
 - vulnerability result, 262

O

- one-armed IDS, 16
- override
 - IPS signature, 84

P

- P2P, 16
- packet logging
 - application control, 206, 214
 - custom IPS overrides, 121
 - IPS, 102, 119
 - settings, 280
 - viewing and saving logged packets, 280
- pattern, 178
 - allow, 178
 - block, 178
 - creating, 179
 - default list of file block patterns, 192
- POP3S
 - antivirus, 278
 - antivirus quarantine, 278
 - data leak prevention, 279
 - DLP archive, 279
 - email filtering, 279
 - predefined firewall services, 277
 - protocol recognition, 278
- predefined firewall services
 - IMAPS, POP3S, SMTPS, 277
- profile group, 289
- protocol decoder, 131
- protocol recognition
 - HTTPS, IMAPS, POP3S, SMTPS, 278

Q

- quarantine, 41
- quarantining attackers to banned user list, 121
- quota
 - FortiGuard Web Filter, 163

R

- regex, 281
- regular expressions, 281

- reports, vulnerability scans
 - creating, 258
 - viewing, 259

S

- scan buffer size
 - antivirus, 38
- scanning order
 - antivirus, 32
- security processing modules
 - configuring, 102
 - example configuration, 111
 - proxy statistics, 114
- sensor
 - IPS, 81
- session count accuracy, 101
- signature
 - adding custom IPS signatures, 85
- signature override
 - IPS, 84
- SMTPS
 - antivirus, 278
 - antivirus quarantine, 278
 - data leak prevention, 279
 - DLP archive, 279
 - email filtering, 279
 - predefined firewall services, 277
 - protocol recognition, 278
- sniffer policies, 16
- sniffer policy
 - viewing, 270
- spam filter
 - banned word list, 72
- spam filter, see email filter, 64
- SSL
 - antivirus, 278
 - antivirus quarantine, 278
 - certificate, 276
 - content inspection, 275
 - content scanning, 275
 - data leak prevention, 279
 - DLP archive, 279
 - email filtering, 279
 - example, 43
 - FortiGuard Web Filtering, 279
 - HTTPS, 279
 - inspection, 275
 - predefined firewall services, 277
 - protocol recognition, 278
 - settings, all, 277
 - supported FortiGate models, 275
 - web filtering, 278
- SYN proxy, 125
- syntax
 - IPS custom signatures, 86

T

- tags
 - application control, 213
 - IPS, 128
 - IPS filters, 120

U

- Unified Threat Management, **see** UTM
- upgrading protocol decoder list, 131
- URL block
 - web filter, 153
- URL filtering, 16
- URL formats, 156
- UTM
 - overview, 15
 - VDOM, 273
- UTM profiles, 17

V

- VDOM
 - UTM, 273
- viewing
 - antivirus list, 115
 - banned word list, 72
 - predefined signatures, 127
- virus database, 36, 47
- virus list, 115
- virus protection. **See** antivirus
- virus scan, 32, 35

vulnerability scan

- adding assets manually, 250
- configuring scans, 253
- creating reports, 258
- discovering assets, 249
- selecting assets to scan, 249
- viewing executive summary graphs, 258
- viewing reports, 259
- viewing results, 253, 257
- viewing scan logs, 257

W

- warning to install FortiClient, 226
- web content filtering, 16
- web filter, 64
 - how URL formats are detected, HTTP, 156
 - how URL formats are detected, HTTPS, 156
 - local ratings, 157
 - quota, 163
 - URL block, 153
 - URL filter, 153
- web filter profile, 147
- web filtering, 16
 - HTTPS, 278
- web monitor, 292
- web-based manager
 - filter settings, 271
- wildcard, 178
- wildcards, 281

